

GALOIS p -GROUPS AND GALOIS MODULES

SUNIL CHEBOLU, JÁN MINÁČ, AND ANDREW SCHULTZ

Dedicated to Professor Albrecht Pfister.

ABSTRACT. The smallest non-abelian p -groups play a fundamental role in the theory of Galois p -extensions. We illustrate this by highlighting their role in the definition of the norm residue map in Galois cohomology. We then determine how often these groups — as well as other closely related, larger p -groups — occur as Galois groups over given base fields. We show further how the appearance of some Galois groups forces the appearance of other Galois groups in an interesting way.

1. INTRODUCTION

From the very beginning Galois theory carries an aura of mystery and depth. Despite some remarkable progress, some very basic problems remain open. Given a base field F and a finite group G , the inverse Galois problem asks whether there is a Galois extension K/F with Galois group G . Even when F is the field of rational numbers we do not know an answer for all G . However in the remarkable paper [46], I.R. Shafarevich showed that each solvable group G appears as a Galois group over any algebraic number field. (See also [47] for corrections related to problems caused by the prime 2.) For the comprehensive treatment of Shafarevich's theorem over any global field, see [39, Sec. 9.6]. For another nice exposition of Shafarevich's theorem in the original case of algebraic number fields, see [18, Ch.V, §6]. For the special case of solvable groups G whose order is a power of a prime p , see [48].

Although in the works above there are some considerable technical issues, some basic principles can be explained briefly. The first basic ingredient is the description of all Galois extensions K/F with Galois group \mathbb{Z}/p over any field F . If F contains a primitive p th root of unity, this problem has a classical, elegant solution described by Kummer theory; if $\text{char}(F) = p$ the problem is solved by Artin-Schreier theory, and when $\text{char}(F) \neq p$ and F does not contain primitive p th root of unity, one can use Galois descent (see [23, Ch. 6]). The appearance of elementary p -abelian groups can be described in this language as well. Indeed, for any field F there exists an \mathbb{F}_p -space $J(F)$ so that subspaces of $J(F)$ of dimension k are in correspondence with elementary p -abelian extensions L/F of rank k . (We will consider $J(F)$ more fully in section 3.)

Date: October 21, 2016.

2010 Mathematics Subject Classification. 12F10 (primary), and 12F12 (secondary).

Key words and phrases. Galois groups, p -groups, Galois modules, enumerating Galois extensions, Norm residue isomorphism.

The first author is partially supported by NSA grant H98230-13-1-0238.

The second author is partially supported by NSERC grant R0370A01.

In order to build a given group G of prime-power order as a Galois group over a given field F , it is natural to consider Galois embedding problems. Consider the short exact sequence

$$1 \longrightarrow \text{Gal}(L/K) \longrightarrow \text{Gal}(L/F) \longrightarrow \text{Gal}(K/F) \longrightarrow 1$$

from Galois theory. If you are given $G \twoheadrightarrow Q$ and you know $\text{Gal}(K/F) \simeq Q$, can you find a Galois extension L/F as above so that $\text{Gal}(L/F) \simeq G$, with the natural map from Galois theory corresponding to the original surjection $G \twoheadrightarrow Q$? This is the Galois embedding problem for $G \twoheadrightarrow Q$ over the extension K/F .

Consider first $p > 2$. The smallest nonabelian groups of prime-power order have order p^3 , and up to group isomorphism there are exactly two such groups (see, e.g., [8, p. 185–186]). The Heisenberg group, which we write H_{p^3} , is the unique nonabelian group of order p^3 and exponent p . This group is isomorphic to $U_3(\mathbb{F}_p)$, the group of upper triangular matrices over a field with p -elements with all diagonal elements 1. The modular group, which we write M_{p^3} , is the unique nonabelian group of order p^3 and exponent p^2 . If $p = 2$ there are also two nonabelian groups of order 8: the dihedral group D_4 (isomorphic to $U_3(\mathbb{F}_2)$) and the quaternion group Q_8 . H_{p^3} and M_{p^3} have the following presentations by generators and relations:

$$\begin{aligned} H_{p^3} &= \langle \sigma, \tau, \omega \mid \sigma^p = \tau^p = \omega^p = [\omega, \sigma] = [\omega, \tau] = \text{id}, [\sigma, \tau] = \omega \rangle \\ M_{p^3} &= \langle x, y \mid y^{p^2} = x^p = \text{id}, [x, y] = y^p \rangle = \langle y \rangle \rtimes \langle x \rangle. \end{aligned} \tag{1}$$

It is worth observing that M_{p^3} is one group in the larger family of groups of the form $M_{p^n} = \langle y : y^{p^{n-1}} = 1 \rangle \rtimes \langle x : x^p = 1 \rangle$. When $p = 2$ and $n > 3$, there are four non-abelian groups of order 2^n which have an element of order 2^{n-1} ; M_{2^n} is obviously one of them, and some automatic realization results for these four groups were considered in [19]. (Jensen uses F_{2^n} to denote the group we're calling M_{2^n} .) For odd p , the group M_{p^n} is the only non-abelian group of order p^n which contains an element of order p^{n-1} (see, e.g., [16, §12.5]). Michailov described in [27] the realizability conditions and Galois extensions for M_{p^n} , as well as several other groups related to this group.

The nonabelian groups of order p^3 , along with the cyclic groups of order dividing p^2 , play a surprising basic role in the structure of some canonical quotients of absolute Galois groups of fields containing a primitive p th root of unity. For $p = 2$, based on work of F. Villegas in [33], it was shown that the fixed field of the third term of the 2-descending central sequence of the absolute Galois group is the compositum of all Galois extensions of the base field with Galois group isomorphic to $\mathbb{Z}/2$, $\mathbb{Z}/4$ or the dihedral group of order 8. Similar results were obtained in [11] for $p > 2$ with groups \mathbb{Z}/p , \mathbb{Z}/p^2 and M_{p^3} . When replacing the 2-descending central sequence by the Zassenhaus descending sequence in [12], an analogous result for groups \mathbb{Z}/p and H_{p^3} was shown. On the other hand, in [7, 12, 13, 34] it was shown that these quotients of absolute Galois groups of fields as above encode crucial information about Galois cohomology, valuations and orderings of fields. These fundamental results can be viewed also as precursors to current investigations in [9, 10, 17, 30, 36, 37, 38] related to Massey products in Galois cohomology.

If F is a field containing a primitive p th root of unity ξ_p , and if $a, b \in F^\times$ give rise to a $\mathbb{Z}/p \times \mathbb{Z}/p$ extension $F(\sqrt[p]{a}, \sqrt[p]{b})/F$, then it is known (see [24, (3.6.4)], [26, Th. 3(A)], [28,

Th. 3.1]) that the embedding problem corresponding to

$$1 \longrightarrow \mathbb{Z}/p \longrightarrow H_{p^3} \longrightarrow \mathbb{Z}/p \times \mathbb{Z}/p \longrightarrow 1 \quad (2)$$

is solvable over $F(\sqrt[p]{a}, \sqrt[p]{b})$ if and only if $b \in N_{F(\sqrt[p]{a})/F}(F(\sqrt[p]{a})^\times)$. The analogous embedding problem for M_{p^3} is solvable over $F(\sqrt[p]{a}, \sqrt[p]{b})$ if and only if $b\xi_p^k \in N_{F(\sqrt[p]{a})/F}(F(\sqrt[p]{a})^\times)$ for some $k \in \mathbb{Z} \setminus p\mathbb{Z}$ (see [26, Cor. p. 523–524], [6, Th. 1] or [28, Th. 3.2].) It is also known that the existence of an extension K/F with $\text{Gal}(K/F) \simeq H_{p^3}$ implies the existence of an extension L/F with $\text{Gal}(L/F) \simeq M_{p^3}$ (see [6, Thm. 2]). In some special cases, more precise results were obtained. Let $\nu(F, G)$ be the number of extensions of F whose Galois group is G (in a fixed algebraic closure \bar{F}), then Brattström has proved ([6, Th. 5]) that when $\text{char}(F) = p$ or $\xi_{p^2} \in F$, one has

$$\nu(F, M_{p^3}) = (p^2 - 1)\nu(F, H_{p^3}).$$

The purpose of this paper is to investigate H_{p^3} , M_{p^3} and their closely related p -groups as Galois groups. We investigate the number of Galois extensions with given Galois group G as above and the interrelation between these numbers. Section 2 discusses the fundamental relation in Galois cohomology. Assume that a and $1 - a$ are non-zero element in a field F and $\xi_p \in F$. Then by Kummer theory we have associated classes $(a), (1 - a) \in H^1(G_F, \mathbb{F}_p)$. Here G_F is the absolute Galois group of F and $H^i(G_F, \mathbb{F}_p)$ is the i th group cohomology of G_F with \mathbb{F}_p -coefficients viewed as a trivial module over G_F . Then $(a) \cup (1 - a) = 0 \in H^2(G_F, \mathbb{F}_p)$, a result known as the Bass-Tate lemma (see Proposition 2.1 below). We discuss how this relation is connected to the solvability of embedding problem (2) over the field $F(\sqrt[p]{a}, \sqrt[p]{1 - a})$. We will use this as motivation for providing an “elementary” proof of this vanishing for $p > 2$ akin to the result of Pfister for $p = 2$ in [40]. Pfister’s proof is remarkable as it uses nothing but the definition of Galois cohomology, but the impetus behind the selection of the desired coboundary is not explained. In our treatment we also keep the elementary nature of the proof, but we shed light on the construction of the desired coboundary.

The Bass-Tate lemma has a fairly short proof (see section 2 below), but it is nevertheless a deep statement which implies automatic realizations for Galois groups H_{p^3} , $\mathbb{Z}/4$ and the dihedral group of order 8. It also connects Galois theory directly to the crucial relation between addition and multiplication in the base field. This connection has some profound consequences for birational anabelian geometry (see [3, 4, 5, 43, 44, 50, 51]).

In section 3 we change our methodology for investigating H_{p^3} and M_{p^3} extensions by replacing the embedding problem from (2) to one that comes from a short exact sequence of the form

$$1 \longrightarrow \mathbb{Z}/p \times \mathbb{Z}/p \longrightarrow G \longrightarrow \mathbb{Z}/p \longrightarrow 1. \quad (3)$$

(Both H_{p^3} and M_{p^3} fit in such an exact sequence.) If K/F is the base extension satisfying $\text{Gal}(K/F) \simeq \mathbb{Z}/p$, this new perspective allows us to parameterize solutions to these embedding problems over K/F by certain $\text{Gal}(K/F)$ -submodules within $J(K)$. This change in perspective also allows us to exhibit H_{p^3} and M_{p^3} within a larger family of p -groups (namely those which can be written as an extension of \mathbb{Z}/p^n by a cyclic $\mathbb{F}_p[\mathbb{Z}/p^n]$ -module) for which the solvability of the associated embedding problem is again tied to the appearance of certain Galois modules in $J(K)$. In the final two sections we use this module-theoretic

perspective to give generalizations of some of the known results concerning the appearance of M_{p^3} and H_{p^3} as Galois groups to this broader family of groups.

1.1. Acknowledgements. We gratefully acknowledge discussions and collaborations with our friends and colleagues I. Efrat, J. Gärtner, S. Gille, D. Hoffmann, J. Labute, J. Swallow, N.D. Tan, A. Topaz, R. Vakil and K. Wickelgren which influenced our thinking and the results presented in this paper. We are also grateful to the referee for his/her valuable suggestions which we used to improve the exposition of this paper.

2. NORM RESIDUE HOMOMORPHISM AND GALOIS MODULES

One of the most exciting theorems from the last decade was the proof of the norm residue isomorphism (previously, the Bloch-Kato conjecture). To state this theorem, we remind the reader of some of important terms. Throughout this section we assume that p is a given prime number and that F is a field which contains a primitive p th root of unity ξ_p . We denote the separable closure of F by F_{sep} and the associated absolute Galois group by $G_F := \text{Gal}(\bar{F}_{\text{sep}}/F)$. When we speak of the cohomology of F , we mean the cohomology groups associated to the trivial G_F -module \mathbb{F}_p : $H^m(F) := H^m(G_F, \mathbb{F}_p)$.

The Milnor K -groups $K_m F$ attached to F are defined as $K_0 F = \mathbb{Z}$, $K_1 F = F^\times$ (the multiplicative group of F), and for $m > 1$ as

$$K_m F := (F^\times)^{\otimes m} / \langle a_1 \otimes \cdots \otimes a_m : \exists 1 \leq i < j \leq m \text{ so that } a_i + a_j = 1 \rangle.$$

Here F^\times is viewed as an abelian group and the tensor product is over \mathbb{Z} . In fact, we obtain a graded ring $K_*(F) = \bigoplus_{m=0}^\infty K_m(F)$ where the product is induced by tensor products. We define the reduced Milnor K -groups as $k_m F := K_m F / \langle p \rangle$, and they too form a graded ring which is also a graded vector space over \mathbb{F}_p . An element of $k_m F$ which is represented by $f_1 \otimes \cdots \otimes f_m$ is written in the form $\{f_1, \dots, f_m\}$. For basic properties of Milnor K -theory we refer the reader to [15, 29, 40, 49].

Now since $\xi_p \in F$ we have $H^1(F) \simeq F^\times / F^{\times p}$, and so it is obvious that $H^1(F)$ and $k_1 F$ are isomorphic. The norm residue isomorphism says that this is true of higher reduced K -groups and cohomology as well, and that this isomorphism respects the underlying ring structures.

The following theorem proved by M. Rost and V. Voevodsky (see [52]) is a substantial advance in Galois cohomology which builds on previous work of J. Arason, H. Bass, S. Bloch, R. Elman, B. Jacob, K. Kato, T.Y. Lam, A. Merkurjev, J. Milnor, A. Suslin, J. Tate and others. See also [41] for a very nice survey concerning this theorem in the case $p = 2$.

Theorem (Norm residue isomorphism). *The rings $k_* F$ and $H^*(F)$ are isomorphic via the map $h : k_* F \rightarrow H^*(F)$ defined by $h(\{f_1, \dots, f_m\}) = (f_1) \cup \cdots \cup (f_m)$.*

Although the following proposition can be proved relatively simply, it is the first step in the long journey of proving the norm residue isomorphism. J. Milnor in [29, p. 339–340] says that this result originated with Bass and Tate.

Proposition 2.1 (Bass-Tate Lemma). *The map $h : k_*F \rightarrow H^*(F)$ is well-defined.*

For this, we need to ensure that the defining relation on the level of K -theory maps to a coboundary in cohomology. In other words, we need to show that if $a \in F^\times \setminus \{1\}$ is given, then the element $(a) \cup (1 - a)$ is trivial in cohomology. Because the standard proof of this result is rather short and interesting, we shall include it here. (See [49, Lem. 8.1] or [15, Sec. 4.6].)

Proof. Because $(b^p) \cup (1 - b^p) = 0$ for all $b \in F^\times$ such that $1 \neq b^p$, we shall assume that $a \notin F^{\times p}$. Since we assume $\xi_p \in F$, we have the factorization $1 - a = \prod_{i=0}^{p-1} (1 - \xi_p^i \sqrt[p]{a})$ in the field $F(\sqrt[p]{a})$. This factorization, however, is equivalent to taking the norm $N_{F(\sqrt[p]{a})/F}(1 - \sqrt[p]{a})$, and so we have

$$(a) \cup (1 - a) = (a) \cup (N_{F(\sqrt[p]{a})/F}(1 - \sqrt[p]{a})).$$

Now the projection formula (see [39, Prop. 1.5.3(iv)]) tells us that when K/F is a Galois extension with $f \in F^\times$ and $k \in K^\times$, then the element $(f) \cup (N_{K/F}(k)) \in H^2(F)$ is equal to $\text{cor}_{K/F}((f) \cup (k))$, where here $\text{cor}_{K/F} : H^2(K) \rightarrow H^2(F)$ is the corestriction map and the element $(f) \cup (k) \in H^2(K)$. Applied to our previous equation, the projection formula gives us

$$\begin{aligned} (a) \cup (1 - a) &= (a) \cup (N_{F(\sqrt[p]{a})/F}((1 - \sqrt[p]{a}))) \\ &= \text{cor}_{F(\sqrt[p]{a})/F}((a) \cup (1 - \sqrt[p]{a})) \\ &= \text{cor}_{F(\sqrt[p]{a})/F}(p(\sqrt[p]{a}) \cup (1 - \sqrt[p]{a})) \\ &= \text{cor}_{F(\sqrt[p]{a})/F}(0) = 0. \end{aligned}$$

□

This proof is certainly elegant, though the critical use of the projection formula prevents us from seeing the result in an “elementary way” (i.e., one which exhibits a given cochain as a coboundary). In the case $p = 2$, Pfister gave just such an elementary proof of the Bass-Tate Lemma in [40]. Our goal in this first section is to prove the vanishing of $(a) \cup (1 - a)$ in two different ways: first by exploiting the known connection between the vanishing of $(x) \cup (y)$ and a particular Galois embedding problem concerning H_{p^3} ; and then by giving an “elementary” proof for $p > 2$ akin to Pfister’s proof for $p = 2$. In fact, in both proofs certain Galois extensions with Galois group H_{p^3} play a key role. If we consider $p = 2$ instead, then the Galois extensions to be considered have Galois group either $\mathbb{Z}/4$ or the dihedral group of order 8.

2.1. A Proof of Bass-Tate via Galois embedding problems. The goal of this next subsection is to give an alternate proof of the vanishing of $(a) \cup (1 - a)$. We shall also assume that $p > 2$, as the case $p = 2$ is similar and no new insight is obtained when considering this case. For the rest of this section we will assume that a and $1 - a$ are independent in $F^\times / F^{\times p}$. This is a reasonable assumption as otherwise $(1 - a) \cup (a)$ vanishes because the cup product is an anticommutative bilinear map $H^1(G_F, \mathbb{F}_p) \times H^1(G_F, \mathbb{F}_p) \rightarrow H^2(G_F, \mathbb{F}_p)$ (see [39, Ch. 1, Sec. 4]). It is possible to shorten our exposition below using [21, Sec. 6.6] or alternatively [28, Th. 3.1] and [42, Ch. 14, Sec. 4, Exer. 2(c)], however we feel that it is instructive to present a detailed full exposition.

We recall (see [24, p. 58]) that for $x, y \in F^\times$, the vanishing of $(x) \cup (y)$ is equivalent to the solvability of the Galois embedding problem

$$1 \longrightarrow \mathbb{F}_p \longrightarrow H_{p^3} \longrightarrow \mathbb{Z}/p \times \mathbb{Z}/p \longrightarrow 1$$

over $F(\sqrt[p]{x}, \sqrt[p]{y})$. Hence we will prove that $(a) \cup (1-a) = 0$ by finding an explicit H_{p^3} -extension of F which contains $L := F(\sqrt[p]{a}, \sqrt[p]{1-a})$ as a quotient. We have already said that the criterion for solving this embedding problem over the field $F(\sqrt[p]{a}, \sqrt[p]{1-a})$ is that $1-a \in N_{F(\sqrt[p]{a})/F}(F(\sqrt[p]{a})^\times)$, and we have already observed this condition in our first proof of Bass-Tate. In a sense, then, we are done. It will be profitable for us to carry the explanation out a bit more completely, however, as this will help us find an explicit representation of $(a) \cup (1-a)$ as a coboundary, and because it is intimately connected to the results we present in subsequent sections.

First, we establish some notation. We know that for $L = F(\sqrt[p]{a}, \sqrt[p]{1-a})$ we have $\text{Gal}(L/F) \simeq \mathbb{Z}/p \times \mathbb{Z}/p$; we will write σ and τ for generators of this group which are dual to a and $1-a$, respectively (e.g., $\sigma(\sqrt[p]{a}) = \xi_p \sqrt[p]{a}$, yet σ acts trivially on $\sqrt[p]{1-a}$). Now consider $\alpha = 1 - \sqrt[p]{a} \in F(\sqrt[p]{a})$. We have already seen that

$$1-a = \prod_{i=0}^{p-1} (1 - \xi_p^i \sqrt[p]{a}) = N_{F(\sqrt[p]{a})/F}(\alpha).$$

We define $\beta = (\sigma - 1)^{p-2}(\alpha)$ and claim that the desired H_{p^3} -extension of L/F is $L(\sqrt[p]{\beta})/F$.

First, observe that the F -conjugates of $\sqrt[p]{\beta}$ are the p th roots of β under the action of σ and τ . Since $\beta \in F(\sqrt[p]{a})$, we have $\tau(\beta) = \beta$. On the other hand, the action of σ on β is nontrivial; because $1 + \sigma + \cdots + \sigma^{p-1} \equiv (\sigma - 1)^{p-1} \pmod{p}$, we have

$$\begin{aligned} \sigma(\beta) &= \sigma((\sigma - 1)^{p-2}\alpha) = \beta(\sigma - 1)^{p-1}\alpha \\ &\equiv \beta N_{F(\sqrt[p]{a})/F}(\alpha) = \beta(1-a) \pmod{F(\sqrt[p]{a})^{\times p}}. \end{aligned}$$

In either case, though, the p th roots of $\tau(\beta)$ and $\sigma(\beta)$ are contained in $L(\sqrt[p]{\beta})$, and hence $L(\sqrt[p]{\beta})$ is Galois.

To prove $\text{Gal}(L(\sqrt[p]{\beta})/F) \simeq H_{p^3}$, begin by noting that this extension is degree p^3 . Hence all we must do is show that this group is noncommutative and that elements have order at most p . Let $\hat{\sigma}$ and $\hat{\tau}$ be lifts of σ and τ to $\text{Gal}(L(\sqrt[p]{\beta})/F)$; it will be enough for us to show that $\hat{\sigma}\hat{\tau} \neq \hat{\tau}\hat{\sigma}$ and that $\hat{\sigma}^p = \hat{\tau}^p = \text{id}$. To arrive at these results, we will only need to investigate actions on $\sqrt[p]{\beta}$ since we already know how $\hat{\tau}$ and $\hat{\sigma}$ act on $\sqrt[p]{a}$ and $\sqrt[p]{1-a}$.

We have already seen that $\hat{\tau}(\beta) = \beta$ and $\hat{\sigma}(\beta) = \beta(1-a)k^p$ for some $k \in F(\sqrt[p]{a})$. By extracting p th roots in these equations, we therefore have

$$\begin{aligned} \hat{\sigma}(\sqrt[p]{\beta}) &= \xi_p^x \sqrt[p]{\beta} \sqrt[p]{1-a} k \\ \hat{\tau}(\sqrt[p]{\beta}) &= \xi_p^y \sqrt[p]{\beta} \end{aligned} \tag{4}$$

for some $x, y \in \mathbb{Z}$. With these identities in hand, it is easy to see that $\hat{\tau}$ and $\hat{\sigma}$ do not commute:

$$\xi_p \hat{\sigma} \hat{\tau}(\sqrt[p]{\beta}) = \hat{\tau} \hat{\sigma}(\sqrt[p]{\beta}).$$

Furthermore by iteratively applying the second part of equation (4), one recovers $\hat{\tau}^p(\sqrt[p]{\beta}) = \sqrt[p]{\beta}$. Hence $\hat{\tau}^p = \text{id}$. On the other hand,

$$\begin{aligned} \frac{\hat{\sigma}^p(\sqrt[p]{\beta})}{\sqrt[p]{\beta}} &= (\hat{\sigma} - 1)(1 + \hat{\sigma} + \hat{\sigma}^2 + \cdots + \hat{\sigma}^{p-1})(\sqrt[p]{\beta}) \\ &= (\hat{\sigma} - 1) \left(\xi_p^z \sqrt[p]{(1 + \sigma + \sigma^2 + \cdots + \sigma^{p-1})\beta} \right) \\ &= (\hat{\sigma} - 1) \left(\xi_p^z \sqrt[p]{N_{F(\sqrt[p]{a})/F}(\beta)} \right) \\ &= (\hat{\sigma} - 1) \left(\xi_p^z \sqrt[p]{1} \right) \\ &= 1. \end{aligned}$$

In this case the second-to-last equality comes from the fact that β is in the image of $\sigma - 1$, and the last equality follows because $\xi_p \in F$ by assumption.

2.2. Exhibiting $(1 - a) \cup (a)$ explicitly as a coboundary. In [40], Pfister gives a very interesting proof of the vanishing of $(a) \cup (1 - a)$ in the case when $p = 2$. Pfister's proof uses nothing but basic definitions from Galois cohomology; he shows that $(a) \cup (1 - a) = 0$ by explicitly exhibiting it as a coboundary. His proof, however, is unmotivated. Where does his choice of coboundary come from? Also, one would like to produce small Galois extensions where one can already define $(a) \cup (1 - a)$ and show that it vanishes there. In our proof below, we explicitly exhibit $(1 - a) \cup (a)$ as a coboundary; there is no significant difference between this and $(a) \cup (1 - a)$ considering the symmetry between a and $1 - a$ and the anti-commutative property of the cup product (see [39, Prop. 1.4.4]). We feel that the vanishing of $(1 - a) \cup (a)$ is in fact a precursor of the n -vanishing Massey conjecture for $n \geq 3$. (See [9, 17, 36, 37, 38] for related material.)

In this section we provide motivation for Pfister's proof, and in the process we both extend it to the case $p > 2$ and show that $(1 - a) \cup (a)$ can be defined on a Galois extension of degree p^3 on which it vanishes. Though thematically similar, there are some small distinctions between the proof when $p > 2$ and $p = 2$; for this reason, we shall focus on the case $p > 2$ and only indicate the necessary changes for $p = 2$. So assume now that $p > 2$.

Before diving into the details, we make a short road map for our argument. Let $\mathbf{p} : F_{\text{sep}}^\times \rightarrow F_{\text{sep}}^\times$ be the map $\mathbf{p}(f) = f^p$; the kernel of this map is $\langle \xi_p \rangle \simeq \mathbb{Z}/p$, and we write η for the associated embedding of \mathbb{Z}/p into F_{sep}^\times . The short exact sequence

$$1 \longrightarrow \mathbb{Z}/p \xrightarrow{\eta} F_{\text{sep}}^\times \xrightarrow{\mathbf{p}} F_{\text{sep}}^\times \longrightarrow 1$$

induces the exact sequence on cohomology

$$H^1(G_F, F_{\text{sep}}^\times) \longrightarrow H^1(G_F, F_{\text{sep}}^\times) \xrightarrow{\delta} H^2(G_F, \mathbb{Z}/p) \xrightarrow{\eta_*} H^2(G_F, F_{\text{sep}}^\times). \quad (5)$$

Although $H^1(G_F, F_{\text{sep}}^\times) = \{0\}$ by Hilbert 90, it is convenient to keep this group in our picture since we need concrete 1-cochains of G_F in F_{sep}^\times . Using the Galois theory of p^3 -extensions, we produce a 1-cochain $N \in C^1(G_F, F_{\text{sep}}^\times)$ such that $d^1(N) = \eta_*((1 - a) \cup (a))$, and hence $\eta_*((1 - a) \cup (a)) = 0$ in $H^2(G_F, F_{\text{sep}}^\times)$. Because η_* is injective, this implies that $(1 - a) \cup (a) = (0) \in H^2(G_F, \mathbb{Z}/p)$. However, in order to produce a specific 2-boundary

for the cochain representing $(1-a) \cup (a)$, we chase sequence (5) and modify N by another 1-cochain M so that $d^1(M)$ is trivial but N/M takes values in \mathbb{Z}/p .

As in the previous section, assume that a and $1-a$ represent classes which are linearly independent in the \mathbb{F}_p -vector space $F^\times/F^{\times p}$. We again write $L = F(\sqrt[p]{a}, \sqrt[p]{1-a})$. Thus L/F is a Galois extension and $\text{Gal}(L/F) \simeq \mathbb{Z}/p \times \mathbb{Z}/p$. We fix a specific primitive p th root of unity ξ_p . This will give us an isomorphism $\iota : \langle \xi_p \rangle \rightarrow \mathbb{Z}/p$; in this way we can identify $\langle \xi_p \rangle$ with \mathbb{Z}/p via ι . Following the convention from section 2.1, we write σ and τ for the generators of $\text{Gal}(L/F)$ that are dual to $\sqrt[p]{a}$ and $\sqrt[p]{1-a}$, respectively.

Observe that $(1-a) \in H^1(G_F, \mathbb{Z}/p)$ is represented by $\gamma \mapsto \iota(\gamma(\sqrt[p]{1-a})/\sqrt[p]{1-a})$, and similarly $(a) \in H^1(G_F, \mathbb{Z}/p)$ is represented by $\gamma \mapsto \iota(\gamma(\sqrt[p]{a})/\sqrt[p]{a})$. Let $\gamma_1, \gamma_2 \in G_F$ restrict to $\tau^i \sigma^k, \tau^l \sigma^j \in \text{Gal}(L/F)$, respectively; we have (see [39, Prop. 1.4.8]) that $(1-a) \cup (a) \in Z^2(G_F, \mathbb{Z}/p)$ is the function

$$(\gamma_1, \gamma_2) \mapsto \iota \left(\frac{\gamma_1(\sqrt[p]{1-a})}{\sqrt[p]{1-a}} \frac{\gamma_2(\sqrt[p]{a})}{\sqrt[p]{a}} \right) = ij \pmod{p}.$$

We now proceed to produce a 1-cochain $h \in C^1(G_F, \mathbb{Z}/p)$ so that $d^1 h(\gamma_1, \gamma_2) = ij \pmod{p}$ (where $d^1 : C^1(G_F, \mathbb{Z}/p) \rightarrow Z^2(G_F, \mathbb{Z}/p)$ is the usual coboundary map). To begin, set $\alpha = 1 - \sqrt[p]{a} \in F(\sqrt[p]{a})$ and $\beta = \alpha^{p-1} \sigma(\alpha^{p-2}) \dots \sigma^{p-2}(\alpha)$. (Note that this element β isn't identical to the element β in section 2.1; see also [21, p. 162].) Note that for the element $x = \sqrt[p]{1-a}/\alpha \in L$ we have $\sigma(\beta)/\beta = x^p$ and

$$x\sigma(x) \dots \sigma^{p-1}(x) = \frac{(\sqrt[p]{1-a})^p}{N_{F(\sqrt[p]{a})/F}(\alpha)} = \frac{1-a}{1-a} = 1. \quad (6)$$

We also have $\tau(x) = \xi_p x$ and $\tau(\beta) = \beta$.

Now let us consider the possible images of β under $\text{Gal}(L/F)$. First, one proves by induction that for any $k \in \{1, \dots, p-1\}$, we have

$$\sigma^k(\beta) = (\sigma^{k-1}(x)\sigma^{k-2}(x) \dots \sigma(x)x)^p \beta.$$

Then since all elements of $\text{Gal}(L/F)$ can be written in the form $\tau^i \sigma^k$, and since we already know that τ acts trivially on x^p and β , this gives all possible images of β under $\text{Gal}(L/F)$. In particular, this means that if $\gamma \in G_F$ restricts to $\tau^i \sigma^k$, then there exists a unique $c \in \{0, 1, \dots, p-1\}$ such that $\gamma(\sqrt[p]{\beta}) = \xi_p^c \sqrt[p]{\beta} \prod_{l=0}^{k-1} \sigma^l(x)$. We use this last equation to define two functions from G_F to F_{sep}^\times :

$$N(\gamma) = \prod_{l=0}^{k-1} \sigma^l(x) \quad \text{and} \quad M(\gamma) = \frac{\gamma(\sqrt[p]{\beta})}{\sqrt[p]{\beta}} = \xi_p^c \prod_{l=0}^{k-1} \sigma^l(x).$$

Note that $M \in Z^1(G_F, F_{\text{sep}}^\times)$ since it is conspicuously in $B^1(G_F, F_{\text{sep}}^\times)$. Observe that using equation (6), one can show that the function $N \in C^1(G_F, F_{\text{sep}}^\times)$ is well-defined. Finally, observe that since

$$\beta \equiv (\sigma - 1)^{p-2}(\alpha) \in F(\sqrt[p]{a})^\times / F(\sqrt[p]{a})^{\times p},$$

section 2.1 tells us that $L(\sqrt[p]{\beta})/F$ is Galois with $\text{Gal}(L(\sqrt[p]{\beta})/F) \simeq H_{p^3}$. Hence M and N are defined on the H_{p^3} -extension $L(\sqrt[p]{\beta})/F$.

As a consequence, we have a 1-cochain $h = \iota_*(N/M) \in C^1(\text{Gal}(L(\sqrt[p]{\beta})/F), \mathbb{Z}/p)$. We show that — as cocycles — we have $\inf(d^1 h) = (1 - a) \cup (a)$. To do this, let us assume that γ_1 and γ_2 are elements of G_F with restrictions in L/F of the form $\tau^i \sigma^k$ and $\tau^l \sigma^j$; our goal will be to show $\inf(d^1 h)(\gamma_1, \gamma_2) = ij \pmod p$. Since $M \in B^1(G_F, F_{\text{sep}})$ we know $d^1 M$ is trivial. Therefore we have

$$\inf\left(d^1 \frac{N}{M}\right)(\gamma_1, \gamma_2) = \iota\left(\frac{N(\gamma_2)^{\gamma_1} N(\gamma_1)}{N(\gamma_1 \gamma_2)} \frac{M(\gamma_1 \gamma_2)}{M(\gamma_2)^{\gamma_1} M(\gamma_1)}\right) = \iota\left(\frac{N(\gamma_2)^{\gamma_1} N(\gamma_1)}{N(\gamma_1 \gamma_2)}\right).$$

By definition we have

$$N(\gamma_1) = \prod_{l=0}^{k-1} \sigma^l(x), \quad N(\gamma_2) = \prod_{l=0}^{j-1} \sigma^l(x), \quad \text{and} \quad N(\gamma_1 \gamma_2) = \prod_{l=0}^{j+k-1} \sigma^l(x).$$

Using the relation $\tau(x) = \xi_p x$ and the fact that σ and τ commute in $\text{Gal}(L/F)$, we recover

$$\begin{aligned} \frac{N(\gamma_2)^{\gamma_1} N(\gamma_1)}{N(\gamma_1 \gamma_2)} &= \left(\prod_{l=0}^{j-1} \sigma^l(x)\right)^{\tau^i \sigma^k} \left(\prod_{l=0}^{k-1} \sigma^l(x)\right) \left(\prod_{l=0}^{j+k-1} \sigma^l(x)\right)^{-1} \\ &= \left(\prod_{l=0}^{j-1} \sigma^l(x^{\tau^i})\right)^{\sigma^k} \left(\prod_{l=0}^{i-1} \sigma^l(x)\right) \left(\prod_{l=0}^{j+k-1} \sigma^l(x)\right)^{-1} = \xi_p^{ij}. \end{aligned}$$

This gives the desired result.

The case $p = 2$ is nearly identical with the case $p > 2$, except that in this case one should consider also the case when $1 - a$ and a belong to the same class in $F^\times/F^{\times 2}$. In this case $L = F(\sqrt{a}, \sqrt{1-a}) = F(\sqrt{a})$ is a quadratic extension and $L(\sqrt{1-\sqrt{a}})/F$ is cyclic of degree 4. When $1 - a$ and a are independent modulo $F^{\times 2}$, the extension $L(\sqrt{a})/F$ is a dihedral extension of degree 8. It is now straightforward to check that the construction above provides a 1-cochain $h \in C^1(G_F, \mathbb{F}_2)$ such that $d^1 h = (a) \cup (1 - a)$ (with (a) and $(1 - a)$ viewed as 1-cochains and $(a) \cup (1 - a)$ viewed as an element of $Z^2(G_F, \mathbb{F}_2)$). Moreover we recover in this way the cochain h introduced by Pfister in [40, p. 275].

3. RECASTING THE EMBEDDING PROBLEM

We continue to assume that p is a prime number, but for the rest of the paper we assume that $p > 2$. We assume that F is a field and K/F an extension with Galois group isomorphic to \mathbb{Z}/p^n . We no longer make assumptions on the characteristic of F or on the roots of unity it contains.

Traditionally, theorems concerning the realizability of H_{p^3} and M_{p^3} as Galois groups are studied from the perspective of embedding problems that arise from group extensions of $\mathbb{Z}/p \times \mathbb{Z}/p$ by \mathbb{Z}/p . In this second part of our paper, we revisit the realizability of these groups as Galois groups by instead studying them as a special case of the family of embedding problems

$$1 \longrightarrow (\mathbb{Z}/p)^{\oplus \ell} \longrightarrow G \longrightarrow \mathbb{Z}/p^n \longrightarrow 1.$$

(Both H_{p^3} and M_{p^3} occur as short exact sequences for $\ell = 2$ and $n = 1$.) By studying appropriate \mathbb{F}_p -vector spaces as modules over Galois groups, we are able to associate the

realizations of these groups as Galois groups to the appearance of modules of a certain type within the classical parameterizing spaces of elementary p -abelian extensions; by using the recently computed module structures for these spaces, we can revisit the known results concerning these groups from this module-theoretic perspective, and furthermore exhibit them as part of a broader phenomena.

We begin by establishing some notation and reminding the reader of some module-theoretic machinery. We write G_n for the group \mathbb{Z}/p^n , and we use σ to denote a generator of this group (the particular n corresponding to σ will be clear from the context).

$\mathbb{F}_p[G_n]$ is a local ring with maximal ideal $\langle \sigma - 1 \rangle$. We define a homomorphism $\psi : \mathbb{F}_p[t] \rightarrow \mathbb{F}_p[G_n]$ by $\psi(t) = \sigma - 1$. Now ψ is a surjective map, and $t^{p^n} \in \ker(\psi)$ because

$$1 = \sigma^{p^n} = ((\sigma - 1) + 1)^{p^n} = (\sigma - 1)^{p^n} + 1.$$

Counting dimensions over \mathbb{F}_p , we conclude that $\mathbb{F}_p[t]/\langle t^{p^n} \rangle \simeq \mathbb{F}_p[G_n]$. Hence we define a “valuation-like” map $v : \mathbb{F}_p[G_n] \rightarrow \mathcal{L}_n$, where $\mathcal{L}_n = \{0, 1, \dots, p^n - 1\} \cup \{\infty\}$ is a set endowed with a binary operation $*$ defined by

$$i * j = \begin{cases} i + j, & \text{if } i, j \neq \infty \text{ and } i + j \leq p^n - 1 \\ \infty, & \text{if } i = \infty \text{ or } j = \infty \text{ or } i + j > p^n - 1. \end{cases}$$

For nonzero $f \in \mathbb{F}_p[G_n]$, we will write $v(f)$ for the maximum value $i \in \mathcal{L}_n \setminus \{\infty\}$ satisfying $f \in \langle (\sigma - 1)^i \rangle$, and we set $v(0) = \infty$. Then we have $v(fg) = v(f) * v(g)$, and $v(f + g) \geq \min\{v(f), v(g)\}$ (following the usual convention that $\infty > i$ for all $i \in \mathcal{L}_n \setminus \{\infty\}$). If M is an $\mathbb{F}_p[G_n]$ -module (written additively) and $\gamma \in M$, then the smallest positive integer ℓ such that $(\sigma - 1)^\ell \gamma = 0$ coincides with the \mathbb{F}_p -dimension of $\langle \gamma \rangle$; we write $\ell(\gamma)$ for this quantity.

If $\gamma_1, \gamma_2 \in M$ and $\mu = \max\{\ell(\gamma_1), \ell(\gamma_2)\}$ we see that

$$(\sigma - 1)^\mu(\gamma_1 + \gamma_2) = (\sigma - 1)^\mu \gamma_1 + (\sigma - 1)^\mu \gamma_2 = 0.$$

Moreover, if $\ell(\gamma_1) < \ell(\gamma_2)$, then for any $\ell(\gamma_1) \leq v < \ell(\gamma_2)$ we have

$$(\sigma - 1)^v(\gamma_1 + \gamma_2) = (\sigma - 1)^v \gamma_1 + (\sigma - 1)^v \gamma_2 = (\sigma - 1)^v \gamma_2 \neq 0.$$

Hence we see that $\ell(\gamma_1 + \gamma_2) \leq \max\{\ell(\gamma_1), \ell(\gamma_2)\}$, with equality if $\ell(\gamma_1) \neq \ell(\gamma_2)$. In what follows, we will refer to this as the ultrametric property.

For $1 \leq \ell \leq p^n$, we define the $\mathbb{F}_p[G_n]$ -module A_ℓ as $\mathbb{F}_p[G_n]/\langle (\sigma - 1)^\ell \rangle$; the action of σ on A_ℓ is simply multiplication by σ . Each of modules from $\{A_\ell\}_{\ell=1}^{p^n}$ is indecomposable, and any indecomposable $\mathbb{F}_p[G_n]$ -module is isomorphic to some A_ℓ . For any $\mathbb{F}_p[G_n]$ -module A there is a unique (unordered) collection of positive integers $\{\ell_i\}_{i \in \mathcal{I}}$ (where possibly $\ell_i = \ell_j$ for $i \neq j$) so that $A \simeq \bigoplus_{i \in \mathcal{I}} A_{\ell_i}$. (For more details, see [31, Sec. 1.1], [25, Sec. 2.3], or [1].)

Remark. The A_ℓ ’s are exactly the indecomposable representations of the cyclic group G_n over the field \mathbb{F}_p .

Remark. By a slight abuse of notation, we denote elements of A_ℓ as elements of $\mathbb{F}_p[G_n]$. In these cases, it should be understood that we intend the given element modulo the ideal of $\mathbb{F}_p[G_n]$ generated by $(\sigma - 1)^\ell$.

3.1. Parameterizing spaces of elementary p -abelian extensions. When K (and therefore F) contains a primitive p th root of unity ξ_p , Kummer theory tells us that elementary p -abelian extensions of K correspond to \mathbb{F}_p -subspaces of $K^\times/K^{\times p}$; these extensions are additionally Galois over F if and only if they are modules over the group ring $\mathbb{F}_p[G_n]$. In this case, we define $J(K) = K^\times/K^{\times p}$.

When K has characteristic p , Artin-Schreier theory gives a correspondence between elementary p -abelian extensions of K and \mathbb{F}_p -subspaces of $K/\wp(K)$, where $\wp(K) = \{k^p - k : k \in K\}$. Again, such an extension is Galois over F if and only if the corresponding \mathbb{F}_p -space is a module over $\mathbb{F}_p[G_n]$. In this case we define $J(K) = K/\wp(K)$.

Finally, if K has characteristic different from p but $\xi_p \notin K$ (and therefore $\xi_p \notin F$), then elementary p -abelian extensions of K correspond to \mathbb{F}_p -subspaces of a particular eigenspace of $K(\xi_p)^\times/K(\xi_p)^{\times p}$. Specifically, if τ is a generator for $\text{Gal}(K(\xi_p)/K)$ and $\tau(\xi_p) = \xi_p^t$, then the space parametrizing elementary p -abelian extensions of K is the subspace on which τ acts as exponentiation by t (the “ t -eigenmodule”). As before, such an extension is Galois over F if and only if the corresponding \mathbb{F}_p -space is a module over the group ring $\mathbb{F}_p[G_n]$ (where here we identify $\text{Gal}(K/F)$ and $\text{Gal}(K(\xi_p)/F(\xi_p))$). In this case, we define $J(K)$ as the t -eigenmodule of $K(\xi_p)^\times/K(\xi_p)^{\times p}$. (These parameterizing spaces are also reviewed in [53].)

It is worth noting that in this latter case, one can describe a morphism \mathcal{T} which projects subspaces of $K(\xi_p)^\times/K(\xi_p)^{\times p}$ to $J(K)$. Let $s = [K(\xi_p) : K]$, and note that $1 < s \leq p-1$. Choose $z \in \mathbb{Z}$ so that $zst^{s-1} \equiv 1 \pmod{p}$, and — again using the notation $\tau(\xi_p) = \xi_p^t$ — set

$$\mathcal{T} = z \sum_{i=1}^s t^{s-i} \tau^{i-1} \in \mathbb{Z}[\langle \tau \rangle]. \quad (7)$$

Notice that $(t - \tau)\mathcal{T} \equiv 0 \pmod{p}$, and so the image of \mathcal{T} is contained in the t -eigenspace for τ . Conversely, if an element is in the t -eigenspace for τ , then \mathcal{T} acts as the identity. Hence we have \mathcal{T} projects \mathbb{F}_p -subspaces of $K(\xi_p)^\times/K(\xi_p)^{\times p}$ onto $J(K)$. (For more details, see [35, Sec. 4] or the proof of [32, Thm. 2].)

Before moving on, we make a brief comment on notation. Our goal is to prove statements about certain embedding problems within the uniform framework provided by $J(K)$. For this reason, whenever we discuss $J(K)$ we will assume it has an underlying additive structure (and therefore $\text{Gal}(K/F)$ acts multiplicatively).

3.2. Module structures and Galois groups. Because $\text{Gal}(K/F)$ induces an action on $J(K)$, it is natural to consider what this additional structure tells us about elementary p -abelian extensions of K . The first answer to this question was given by Waterhouse in [53], where he considered cyclic submodules of $J(K)$ when $\text{char}(K) \neq p$. The question was answered for non-cyclic modules, as well as in the case $\text{char}(K) = p$, by the authors in [32, 45]; there the $\mathbb{F}_p[G_n]$ -module $J(K)$ is exhibited as a parameterizing space for solutions to embedding problems over K/F which arise from extensions of G_n by elementary p -abelian groups. Since we are focusing on groups related to H_{p^3} and M_{p^3} in this paper, it will be sufficient for us to focus our attention on cyclic $\mathbb{F}_p[G_n]$ -submodules.

So let L/K be an elementary p -abelian extension which corresponds to a cyclic $\mathbb{F}_p[G_n]$ -submodule $\langle \gamma \rangle \subseteq J(K)$. Then L/F is Galois and $\text{Gal}(L/F)$ is an extension of $\text{Gal}(K/F) \simeq G_n$ by $\text{Gal}(L/K)$. Using the appropriate parameterizing theory (e.g., Kummer theory if $\text{char}(K) \neq p$ and $\xi_p \in K$), one can show that there is an equivariant pairing $\text{Gal}(L/K) \times \langle \gamma \rangle \rightarrow \mathbb{F}_p$, and hence $\text{Gal}(L/K)$ is dual to $\langle \gamma \rangle$. One can show that $\mathbb{F}_p[G_n]$ -modules are self-dual, and so we conclude that $\text{Gal}(L/F)$ is an extension of $\text{Gal}(K/F) \simeq G_n$ by $\langle \gamma \rangle$.

With this in mind, we now describe the possible extensions of G_n by a cyclic $\mathbb{F}_p[G_n]$ -module.

Proposition 3.1 ([53, Thm. 2]). *There is only one group extension of G_n by A_{p^n} , namely the semi-direct product $A_{p^n} \rtimes G_n$. For $1 \leq i < p^n$ there are two possible group extensions of G_n by A_i . One of them is the semi-direct product $A_i \rtimes G_n$, where we have*

$$(f_1, \sigma^{j_1})(f_2, \sigma^{j_2}) = (f_1 + \sigma^{j_1} f_2, \sigma^{j_1+j_2}).$$

The second extension of G_n by A_i will be written $A_i \bullet G_n$; the elements of this group again come from $A_i \times G_n$, but the operation is given by

$$(f_1, \sigma^{j_1})(f_2, \sigma^{j_2}) = \begin{cases} (f_1 + \sigma^{j_1} f_2, \sigma^{j_1+j_2}) & , \text{ if } j_1 + j_2 < p^n \\ (f_1 + \sigma^{j_1} f_2 + (\sigma - 1)^{i-1}, \sigma^{j_1+j_2}) & , \text{ if } j_1 + j_2 \geq p^n. \end{cases}$$

(Here the numbers j_1 and j_2 are taken from $\{0, \dots, p^n - 1\}$.)

Example 3.2. Let $\sigma, \tau \in H_{p^3}$ be nontrivial elements which generate H_{p^3} . Then we have $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ is an element of order p which generates $Z(H_{p^3})$. Now consider the $\mathbb{F}_p[\langle \sigma \rangle]$ -module B which is the \mathbb{F}_p -span of $\{\tau, [\sigma, \tau]\}$ (where the action of σ is by conjugation). The computation $(\sigma - 1) \cdot \tau = \sigma\tau\sigma^{-1}\tau^{-1} = [\sigma, \tau]$ shows that $\langle \tau \rangle = B$ as an $\mathbb{F}_p[\langle \sigma \rangle]$ -module, and so $B \simeq A_2$. Because $\langle \sigma \rangle \cap B = \{1\}$ and $\langle \sigma \rangle \simeq G_1$, we conclude that $H_{p^3} \simeq A_2 \rtimes G_1$. Phrased in a slightly different language, this example tells us that if N is any subgroup of H_{p^3} with $|N| = p^2$ and $Q := H_{p^3}/N$, then $N \simeq A_2$ as an $\mathbb{F}_p[Q]$ -module and $H_{p^3} \simeq N \rtimes Q$.

Now recall that $M_{p^3} = \langle y, x \mid y^{p^2} = x^p = 1, [x, y] = y^p \rangle = \langle y \rangle \rtimes \langle x \rangle$. The subgroups $\langle y^k x \rangle$ for $k \in \{1, \dots, p-1\}$, together with the subgroup $\langle y \rangle$, provide p distinct subgroups isomorphic to \mathbb{Z}/p^2 . On the other hand, we claim that the subgroup $N = \langle y^p, x \rangle$ can be the only subgroup of M_{p^3} isomorphic to $\mathbb{Z}/p \times \mathbb{Z}/p$. To see this, note that the p subgroups isomorphic to \mathbb{Z}/p^2 provide us with $p \cdot \phi(p^2) = p^3 - p^2$ elements of order p^2 , and so the number of elements of order less than p^2 within M_{p^3} is at most p^2 . Since N already contains p^2 elements of this type, it can be the only subgroup isomorphic to $\mathbb{Z}/p \times \mathbb{Z}/p$. On the other hand, a direct computation shows that $[y^p, x] = 1$, so that $N \simeq \mathbb{Z}/p \times \mathbb{Z}/p$.

Now let $Q = M_{p^3}/N = \langle yN \rangle \simeq G_1$. We have that N is generated by x under the action of yN , and hence $N \simeq A_2$ as an $\mathbb{F}_p[G_1]$ -module. In this case, however, one has $M_{p^3} \simeq A_2 \bullet G_1$ (one can verify this directly, or simply note that $A_2 \rtimes G_1$ has no elements of order p^2).

Example 3.3. Let $n \geq 3$, and consider the group $A_2 \bullet G_{n-2}$. Using the notation from the previous proposition, we have

$$\begin{aligned} (0, \sigma)^{p^{n-2}} &= (\sigma - 1, 1) \\ (0, \sigma)^{p^{n-1}} &= \left((0, \sigma)^{p^{n-2}} \right)^p = (\sigma - 1, 1)^p = (0, 1). \end{aligned}$$

Hence $A_2 \bullet G_{n-2}$ is a nonabelian p -group with order p^n that contains an element of order p^{n-1} . Since we've already observed that there is only one such p -group — which we previously called M_{p^n} — we must have $M_{p^n} \simeq A_2 \bullet G_{n-2}$.

If L/K corresponds to $\langle \gamma \rangle$, all that is left to do is determine which extension of G_n by $\langle \gamma \rangle$ corresponds to $\text{Gal}(L/F)$. To do this, one uses the so-called index function. The index is a function $e : J(K) \cap \ker((\sigma - 1)^{p^{n-1}}) \rightarrow \mathbb{F}_p$ defined by

$$e(\gamma) = \begin{cases} \sqrt[p]{N_{\hat{K}/\hat{F}}(\gamma)}^{\sigma^{-1}}, & \text{if } \text{char}(K) \neq p \\ (\sigma - 1)\rho(\text{Tr}_{K/F}(\gamma)), & \text{if } \text{char}(K) = p. \end{cases}$$

(In the first case we have identified μ_p with \mathbb{F}_p by selecting a particular root of unity ξ_p to act as a generator of μ_p .) With the index in hand, we have the following

Proposition 3.4 ([45], Thm. 4.4). *Suppose $\text{Gal}(K/F) \simeq G_n$. Solutions to the embedding problem $A_{p^n} \rtimes G_n \rightarrow G_n$ are in correspondence with submodules $\langle \gamma \rangle \subseteq J(K)$ such that $\ell(\gamma) = p^n$. For $i < p^n$, solutions to the embedding problem $A_i \rtimes G_n \rightarrow G_n$ over K/F are in correspondence with the submodules $\langle \gamma \rangle \subseteq J(K)$ such that $\ell(\gamma) = i$ and $e(\gamma) = 0$; solutions to the embedding problem $A_i \bullet G_n \rightarrow G_n$ over K/F are in correspondence with the submodules $\langle \gamma \rangle \subseteq J(K)$ such that $\ell(\gamma) = i$ and $e(\gamma) \neq 0$.*

Example 3.5. Suppose that L/F has $\text{Gal}(L/F) \simeq H_{p^3}$, and let K/F be any \mathbb{Z}/p -subextension. Then L/K is Galois with $\text{Gal}(L/K) \simeq \mathbb{Z}/p \times \mathbb{Z}/p$, and hence L corresponds to some submodule $M \subseteq J(K)$. Since $\text{Gal}(L/F)$ is nonabelian it must be the case that $M \not\subseteq A_1 \oplus A_1$, and so $M \simeq A_2$. If $\langle \gamma \rangle = M$, we must have $e(\gamma) = 0$ by the previous proposition. Conversely, if K/F is an extension with $\text{Gal}(K/F) \simeq \mathbb{Z}/p$ and $\langle \gamma \rangle \subseteq J(K)$ satisfies $\ell(\gamma) = 2$ and $e(\gamma) = 0$, then $\langle \gamma \rangle$ corresponds to an extension L/K with $\text{Gal}(L/F) \simeq H_{p^3}$.

Suppose now that L/F has $\text{Gal}(L/F) \simeq M_{p^3}$. Then there is a unique subextension K/F with $\text{Gal}(K/F) \simeq \mathbb{Z}/p$ and $\text{Gal}(L/K) \simeq \mathbb{Z}/p \times \mathbb{Z}/p$. Within $J(K)$ there exists a submodule M corresponding to L/K , and again it must be the case that $M = \langle \gamma \rangle$ with $\ell(\gamma) = 2$ and $e(\gamma) \neq 0$. Conversely, if K/F is an extension with $\text{Gal}(K/F) \simeq \mathbb{Z}/p$ and $\langle \gamma \rangle \subseteq J(K)$ satisfies $\ell(\gamma) = 2$ and $e(\gamma) \neq 0$, then $\langle \gamma \rangle$ corresponds to an extension L/F containing K with $\text{Gal}(L/F) \simeq M_{p^3}$.

The structure of $J(K)$ was computed when $\xi_p \in K$ in [31, Thm. 2], when $\xi_p \notin K$ but $\text{char}(K) \neq p$ in [32, Thm. 2], and when $\text{char}(K) = p$ in [45, Prop. 6.2]. (Note that in the case of $\text{char}(K) = p$ and $\xi_p \notin F$, there is a module decomposition for $K^\times/K^{\times p}$ provided by [31, Thm. 1]; in this case, however, $J(K) \neq K^\times/K^{\times p}$, so this is not the decomposition we provide below.) Though there are some distinctions between the structure of $J(K)$ in these cases, certain qualitative information about these modules is common in all cases. We summarize the important characteristics in the following

Proposition 3.6. *If $\text{Gal}(K/F) \simeq G_n$, then $J(K) = \langle \chi \rangle \oplus \bigoplus_{i=0}^n Y_i$, where*

- $\ell(\chi) = p^{i(K/F)} + 1$ for some $i(K/F) \in \{-\infty, 0, 1, \dots, n-1\}$, and $e(\chi) \neq 0$; and
- for each $0 \leq i \leq n$ there exists \mathfrak{d}_i so that $Y_i \simeq \bigoplus_{\mathfrak{d}_i} \mathbb{F}_p[G_i]$, and if $i < n$ then $Y_i \subseteq \ker e$.

The invariant $i(K/F)$ from this theorem has a variety of interpretations, though there are two that are important for our purposes. The first has an embedding problem flavor. If K/F embeds in a cyclic extension of degree p^{n+1} , then $i(K/F) = -\infty$. Otherwise, write K_i for the subextension of degree p^i over F , and choose s minimally so that K/K_s embeds in a cyclic extension of degree p^{n-s+1} ; then $i(K/F) = s - 1$. Note in particular that $i(K/F) = -\infty$ whenever $\text{char}(K) = p$, since Witt's Theorem on embedding problems in characteristic p ([55]) tells us that any \mathbb{Z}/p^n -extension embeds in a \mathbb{Z}/p^{n+1} -extension in this setting. The second interpretation of $i(K/F)$ concerns the dimensions of modules generated by elements with nontrivial index: if $e(\gamma) \neq 0$, then $\ell(\gamma) \geq \ell(\chi) = p^{i(K/F)} + 1$.

In light of this correspondence, one of the immediate observations to make from Proposition 3.6 is the following.

Corollary 3.7 (cf. [11, Prop. 10.2]). *If K/F is a \mathbb{Z}/p -extension, then either $\mathbb{Z}/p^2 \twoheadrightarrow \mathbb{Z}/p$ or $M_{p^3} \twoheadrightarrow \mathbb{Z}/p$ is solvable over K/F . More generally, if K/F is a \mathbb{Z}/p^n -extension, then for some $i \in \{-\infty, 0, 1, \dots, n-1\}$ the embedding problem $A_{p^i+1} \bullet \mathbb{Z}/p^n \twoheadrightarrow \mathbb{Z}/p^n$ is solvable over K/F .*

Proof. By Proposition 3.6 there exists an element $\chi \in J(K)$ so that $e(\chi) \neq 0$ and $\ell(\chi) = p^{i(K/F)} + 1$ for some $i(K/F) \in \{-\infty, 0, 1, \dots, n-1\}$. By Proposition 3.4 this module corresponds to a solution to the embedding problem $A_{p^{i(K/F)}+1} \bullet G_n \twoheadrightarrow G_n$. \square

Corollary 3.8. *If K/F is a \mathbb{Z}/p^n -extension so that for some $j > i$ both $A_i \bullet \mathbb{Z}/p^n \twoheadrightarrow \mathbb{Z}/p^n$ and $A_j \bullet \mathbb{Z}/p^n \twoheadrightarrow \mathbb{Z}/p^n$ are solvable over K/F , then $A_j \rtimes \mathbb{Z}/p^n \twoheadrightarrow \mathbb{Z}/p^n$ is also solvable over K/F .*

Proof. Solutions to the embedding problems $A_i \bullet G_n \twoheadrightarrow G_n$ and $A_j \bullet G_n \twoheadrightarrow G_n$ correspond to elements $\gamma_i, \gamma_j \in J(K)$ with nontrivial index and satisfying $\ell(\gamma_i) = i$ and $\ell(\gamma_j) = j$. By choosing an appropriate $c \in \mathbb{Z} \setminus p\mathbb{Z}$, one has $e(c\gamma_i + \gamma_j) = 0$; furthermore $\ell(c\gamma_i + \gamma_j) = j$ by the ultrametric property. Hence $\langle c\gamma_i + \gamma_j \rangle$ corresponds to a solution to $A_j \rtimes G_n \twoheadrightarrow G_n$. \square

Remark. One cannot make this statement stronger by saying that the appearance of $A_i \bullet G_n$ and $A_j \bullet G_n$ over a field F forces the appearance of $A_j \rtimes G_n$ over F since there are fields F which admit both $\mathbb{Z}/p^2 \simeq A_1 \bullet G_1$ - and $M_{p^3} \simeq A_2 \bullet G_1$ -extensions, but which do not admit an $H_{p^3} \simeq A_2 \rtimes G_1$ -extension. See, for example, [6, p. 167].

4. AUTOMATIC REALIZATIONS RELATED TO $H_{p^3} \Rightarrow M_{p^3}$

The last two results show that the appearance of certain groups as Galois groups over a field F can force the appearance of other groups as Galois groups over F as well in a non-trivial way. In this section we will consider other results in this vein. For a group G and a field F , we write $\nu(G, F)$ for the number of extensions L/F with $\text{Gal}(L/F) \simeq G$ in

a fixed algebraic closure of F . In the same way, $\nu(G \twoheadrightarrow Q, K/F)$ counts the number of solutions L/F to a given embedding problem $G \twoheadrightarrow Q$ over K/F .

A group G is said to automatically realize a group H if $\nu(G, F) > 1$ implies $\nu(H, F) > 1$ for any field F . The classic automatic realization theorem is Whaples' result [54] that if p is an odd prime number, then \mathbb{Z}/p^i automatically realizes \mathbb{Z}/p^j for all $i < j$. One can also consider automatic realizations for embedding problems: $G \twoheadrightarrow Q$ is said to automatically realize $H \twoheadrightarrow Q$ if $\nu(G \twoheadrightarrow Q, K/F) \geq 1$ implies $\nu(H \twoheadrightarrow Q, K/F) \geq 1$.

Brattström was the first to consider automatic realizations between H_{p^3} and M_{p^3} in [6]. She showed that H_{p^3} automatically realizes M_{p^3} [6, Th. 2], and that M_{p^3} does not automatically realize H_{p^3} in general [6, p. 167]. (The fact that H_{p^3} automatically realizes M_{p^3} was also proved in a different way in [11, Cor. 12].) However, she does argue that the solvability of the embedding problem $M_{p^3} \twoheadrightarrow G_1$ over a field K/F will imply the solvability of the embedding problem $H_{p^3} \twoheadrightarrow G_1$ over K/F if either $\text{char}(K) = p$ or $\xi_p \in N_{K/F}(K^\times)$ [6, Th. 2]. (There are some other known automatic realization results associated with H_{p^3} and M_{p^3} . For instance, in [20, Th. 1.4A] it was observed that for any finite group G , the group $H_{p^3} \times G$ automatically realizes $M_{p^3} \times G$. In [20, Prop. 1.5] it was also observed that if

$$A = \langle x, y | x^{p^2} = y^{p^2} = 1, xy = yx^{1+p} \rangle,$$

then M_{p^3} automatically realizes A .)

By interpreting H_{p^3} as $A_2 \rtimes G_1$ and M_{p^3} as $A_2 \bullet G_1$, we now show Brattström's results can be viewed from the perspectives of Propositions 3.4 and 3.6. Indeed, if the embedding problem $A_2 \rtimes G_1 \twoheadrightarrow G_1$ is solvable, then there exists $\langle \gamma \rangle \subseteq J(K)$ with $\ell(\gamma) = 2$ and $e(\gamma) = 0$. Using the notation of Proposition 3.6, if $\ell(\chi) = 2$, then $\langle \chi \rangle$ corresponds to a solution to $A_2 \bullet G_1 \twoheadrightarrow G_1$ and we are done. Otherwise $\ell(\chi) = 1$, and so $\ell(\gamma + \chi) = 2$ by the ultrametric property. Since $e(\gamma + \chi) = e(\chi) \neq 0$, it therefore follows that $\langle \gamma + \chi \rangle$ corresponds to a solution to $A_2 \bullet G_1 \twoheadrightarrow G_1$ over K/F .

On the other hand, suppose that L/F is an M_{p^3} -extension, and let K/F be the unique \mathbb{Z}/p -subextension. If we assume $\xi_p \in N_{K/F}(K^\times)$ then by a famous result of Albert we know that K/F embeds in a \mathbb{Z}/p^2 -extension, whereas if $\text{char}(F) = p$ then it's Witt's theorem which tells us that K/F embeds in a \mathbb{Z}/p^2 -extension. In either case we conclude that χ from Proposition 3.6 must satisfy $\ell(\chi) = 1$. Now let $\langle \gamma \rangle$ correspond to the given M_{p^3} extension. Then $\ell(\gamma) = 2$ and $e(\gamma) \neq 0$. By choosing an appropriate $c \in \mathbb{Z} \setminus p\mathbb{Z}$, one has $e(\gamma + c\chi) = 0$ and $\ell(\gamma + c\chi) = 2$. Hence this element corresponds to a solution to $A_2 \rtimes G_1 \twoheadrightarrow G_1$.

Using this same line of reasoning, we fit this result into a family of similar results which we phrase in the slightly stronger language of automatic realizations of embedding problems.

Proposition 4.1. *We have the following automatic realization results:*

- (1) $A_\ell \rtimes G_n \twoheadrightarrow G_n$ automatically realizes $A_{\ell+1} \rtimes G_n \twoheadrightarrow G_n$ for $\ell \neq p^k$ with $k \in \{0, 1, \dots, n-1\}$;
- (2) $A_\ell \bullet G_n \twoheadrightarrow G_n$ automatically realizes $A_\ell \rtimes G_n \twoheadrightarrow G_n$ for $\ell \neq p^k + 1$ with $k \in \{0, 1, \dots, n-1\}$;

- (3) $A_\ell \bullet G_n \twoheadrightarrow G_n$ automatically realizes $A_{\ell-1} \bullet G_n \twoheadrightarrow G_n$ for $\ell \neq p^k + 1$ with $k \in \{0, 1, \dots, n-1\}$; and
 (4) $A_{p^{n-1}+1} \rtimes G_n \twoheadrightarrow G_n$ automatically realizes $A_{p^{n-1}+k} \bullet G_n \twoheadrightarrow G_n$ for $1 \leq k < p^n - p^{n-1}$.

Proof. (1) was essentially the subject of [32], but we reprove the result here. A solution to the embedding problem $A_\ell \rtimes G_n \twoheadrightarrow G_n$ corresponds to a submodule $\langle \gamma \rangle \subseteq J(K)$ with $\ell(\gamma) = \ell$ and $e(\gamma) = 0$. By Proposition 3.6 we can find an $\mathbb{F}_p[G_n]$ -basis $\{\chi\} \cup \{\alpha_i\}_{i \in \mathcal{I}}$ for $J(K)$ so that $e(\chi) \neq 0$ and $\ell(\chi) = p^i(K/F) + 1$, and so that for all $i \in \mathcal{I}$ we have $\ell(\alpha_i) = p^{\ell_i}$ for $\ell_i \in \{0, \dots, n\}$ and $e(\alpha_i) = 0$ when $\ell(\alpha_i) < p^n$. Express

$$\gamma = f\chi + \sum_{i \in \mathcal{I}} f_i \alpha_i$$

with $f, f_i \in \mathbb{F}_p[G_n]$; since $e(\gamma) = 0$, it must be the case that $f \in \langle \sigma - 1 \rangle$; likewise since $\ell(\gamma) = \ell < p^n$ we must have $f_i \in \langle \sigma - 1 \rangle$ for all $i \in \mathcal{I}$ such that $\ell(\alpha_i) = p^n$. Now we have $\ell(\gamma) = \max\{\ell(f\chi), \{\ell(f_i \alpha_i) : i \in \mathcal{I}\}\}$ using the ultrametric property together with the $\mathbb{F}_p[G_n]$ -independence of the set $\{\chi\} \cup \{\alpha_i\}_{i \in \mathcal{I}}$.

We consider two cases. If $\ell(\gamma) = \ell(f\chi)$, then since $\ell \neq p^k$ for any $k \in \{0, 1, \dots, n-1\}$ and $\ell(f\chi) = p^{i(K/F)} + 1 - v(f)$, we must have $v(f) \geq 2$. Hence $\ell((\sigma - 1)^{v(f)-1}\chi) = \ell + 1$ and $e((\sigma - 1)^{v(f)-1}\chi) = 0$. Hence $A_{\ell+1} \rtimes G_n \twoheadrightarrow G_n$ has a solution.

On the other hand, if $\ell(\gamma) = \ell(f_i \alpha_i)$ for some $i \in \mathcal{I}$, then since $\ell(\alpha_i) = p^{\ell_i}$, it must be the case that $v(f_i) \geq 1$. But then $\ell((\sigma - 1)^{v(f_i)-1}\alpha_i) = \ell + 1$ and $e((\sigma - 1)^{v(f_i)-1}\alpha_i) = 0$. Again, we have a solution to $A_{\ell+1} \rtimes G_n \twoheadrightarrow G_n$.

(2) has two potential proofs. From the group-theoretic perspective, $A_{\ell-1} \rtimes G_n$ is a quotient of $A_\ell \bullet G_n$, and hence $A_\ell \bullet G_n \twoheadrightarrow G_n$ trivially automatically realizes $A_{\ell-1} \rtimes G_n \twoheadrightarrow G_n$. Then (1) tells us that $A_{\ell-1} \rtimes G_n \twoheadrightarrow G_n$ automatically realizes $A_\ell \rtimes G_n \twoheadrightarrow G_n$. Alternatively, one could prove this result module-theoretically. In this case, a solution to $A_\ell \bullet G_n \twoheadrightarrow G_n$ implies the existence of a submodule $\langle \gamma \rangle \subseteq J(K)$ with $\ell(\gamma) = \ell$ and $e(\gamma) \neq 0$. Choose an appropriate value $c \in \mathbb{Z} \setminus p\mathbb{Z}$ so that $e(c\chi + \gamma) = 0$, and note that $\ell(c\chi + \gamma) = \ell(\gamma)$ by the ultrametric property (recall that if $e(\gamma) \neq 0$ then $\ell(\gamma) \geq \ell(\chi)$, and our hypothesis forces this inequality to be strict). Hence $\langle c\chi + \gamma \rangle$ corresponds to a solution to $A_\ell \rtimes G_n \twoheadrightarrow G_n$.

For the proof of (3), suppose that $\langle \gamma \rangle \subseteq J(K)$ corresponds to a solution to the embedding problem $A_\ell \bullet G_n \twoheadrightarrow G_n$. The module-theoretic proof of (2) gives us a module $\langle c\chi + \gamma \rangle$ with $e(c\chi + \gamma) = 0$ and $\ell = \ell(c\chi + \gamma) > \ell(\chi)$. If $\ell(\chi) = \ell - 1$, then $\langle \chi \rangle$ corresponds to a solution to the embedding problem $A_{\ell-1} \bullet G_n \twoheadrightarrow G_n$. Otherwise $\ell(\chi + (\sigma - 1)(c\chi + \gamma)) = \ell - 1$, and of course this module is generated by an element of nontrivial index. Hence it corresponds to a solution to the embedding problem $A_{\ell-1} \bullet G_n \twoheadrightarrow G_n$.

Finally, to prove (4), we use (1) to conclude that there is a solution to $A_{p^{n-1}+k} \rtimes G_n \twoheadrightarrow G_n$ over K/F . Write $\langle \gamma \rangle \subseteq J(K)$ for the module that corresponds to a solution to the embedding problem $A_{p^{n-1}+k} \rtimes G_n \twoheadrightarrow G_n$. Obviously $e(\chi + \gamma) \neq 0$, and if we can show $\ell(\chi + \gamma) = p^{n-1} + k$ then this module will correspond to a solution to the embedding problem $A_{p^{n-1}+k} \bullet G_n \twoheadrightarrow G_n$. We know that $\ell(\chi + \gamma) \leq \max\{p^{n-1} + k, p^{i(K/F)} + 1\} = p^{n-1} + k$, with equality if either $k > 1$ or $i(K/F) \neq n - 1$. Hence $\ell(\chi + \gamma) < p^{n-1} + k$ implies both $k = 1$ and $i(K/F) = n - 1$. But since $e(\chi + \gamma) \neq 0$ and χ is an element of minimal length amongst

elements of non-trivial index, we must also have $p^{n-1} + 1 > \ell(\chi + \gamma) \geq \ell(\chi) = p^{n-1} + 1$, a contradiction. \square

Finally, we give a proposition which builds on Proposition 4.1(4), but doesn't require the underlying $\mathbb{F}_p[G_n]$ -module to have such a large dimension. Recall that K_i denotes the intermediate field in the extension K/F such that $[K_i : F] = p^i$.

Proposition 4.2. *Let $i \in \{0, 1, \dots, n-1\}$ be given. If the embedding problems $G_{n-i} \twoheadrightarrow G_{n-i-1}$ over K/K_{i+1} and $A_{p^{i+1}} \rtimes G_n \twoheadrightarrow G_n$ over K/F are both solvable, then the embedding problem $A_{p^{i+k}} \bullet G_n \twoheadrightarrow G_n$ is also solvable over K/F for all $1 \leq k \leq p^{i+1} - p^i$.*

Proof. The proof of this result is essentially the same as the proof of Proposition 4.1(4), though our additional hypothesis concerning the solvability of $G_{n-i} \twoheadrightarrow G_{n-i-1}$ over K/K_{i+1} tells us that $i(E/F) \leq i$, so that $\ell(\chi) \leq p^i + 1$. To find a solution to the desired embedding problem, we note that the solvability of $A_{p^{i+1}} \rtimes G_n \twoheadrightarrow G_n$ over K/F implies the solvability of $A_{p^{i+k}} \rtimes G_n \twoheadrightarrow G_n$ over K/F ; let $\langle \gamma \rangle$ be a module in $J(K)$ which corresponds to a solution to this embedding problem. Then the module $\langle \gamma + \chi \rangle$ will be a solution to the embedding problem $A_{p^{i+k}} \bullet G_n \twoheadrightarrow G_n$. \square

5. ENUMERATING GALOIS EXTENSIONS RELATED TO H_{p^3} AND M_{p^3}

We now shift focus and concentrate on enumeration results related to H_{p^3} and M_{p^3} , particularly within the family of groups $A_i \rtimes G_1$ and $A_i \bullet G_1$. One of the results already known in this vein comes from a paper by Brattström ([6, Thm. 5]) where it is shown that

$$\nu(M_{p^3}, F) = (p^2 - 1)\nu(H_{p^3}, F) \quad \text{if } \xi_{p^2} \in F \text{ or } \text{char}(F) = p.$$

Here we present a stronger result that drops the assumption that $\xi_{p^2} \in F$ when $\text{char}(F) \neq p$ and gives a closed formula for the difference $\nu(M_{p^3}, F) - (p^2 - 1)\nu(H_{p^3}, F)$.

Before arriving at this result, we will first need to consider the following \mathbb{F}_p -subspace of $J(F)$:

$$\mathfrak{N} = \begin{cases} \frac{N_{F(\xi_{p^2})/F}(F(\xi_{p^2})^\times) \cdot F^{\times p}}{F^{\times p}}, & \text{when } \xi_p \in F \\ J(F), & \text{when } \text{char}(F) = p \\ \mathcal{T} \left(\frac{N_{F(\xi_{p^2})/F(\xi_p)}(F(\xi_{p^2})^\times) \cdot F(\xi_p)^{\times p}}{F(\xi_p)^{\times p}} \right), & \text{when } \text{char}(F) \neq p \text{ and } \xi_p \notin F. \end{cases}$$

Recall that in the latter case we write τ for the generator of $\text{Gal}(F(\xi_p)/F)$, and that $\mathcal{T} \in \mathbb{Z}[\langle \tau \rangle]$. Because $\gcd(|\tau|, p) = 1$, we have that

$$(N_{F(\xi_{p^2})/F(\xi_p)}(\alpha))^\tau = N_{F(\xi_{p^2})/F(\xi_p)}(\alpha^\tau)$$

for any $\alpha \in F(\xi_{p^2})^\times$. It follows that \mathfrak{N} is the t -eigenspace for τ within $\frac{N_{F(\xi_{p^2})/F(\xi_p)}(F(\xi_{p^2})^\times) \cdot F(\xi_p)^{\times p}}{F(\xi_p)^{\times p}}$. The importance of this space is that it parameterizes those elements of $J(F)$ whose corresponding G_1 -extensions admit a solution to the embedding problem $G_2 \twoheadrightarrow G_1$.

Proposition 5.1. *Suppose that $f \in J(F)$ corresponds to the \mathbb{Z}/p -extension K/F . Then the embedding problem $G_2 \twoheadrightarrow G_1$ has a solution over K/F if and only if $f \in \mathfrak{N}$.*

Proof. This result is [2, Thm. 1] if $\xi_p \in F$; when $\xi_p \notin F$ and $\text{char}(F) \neq p$, the result follows by descent. If $\text{char}(F) = p$ then the embedding problem $G_2 \twoheadrightarrow G_1$ is always solvable. \square

We are now prepared to give a generalization of Brattström's result connecting $\nu(H_{p^3}, F)$ and $\nu(M_{p^3}, F)$. In the statement of this theorem, we use $\binom{n}{m}_p$ for the p -binomial coefficient which counts the number of m -dimensional subspaces within an ambient n -dimensional \mathbb{F}_p -space. It is a nice exercise in linear algebra to show that

$$\binom{n}{m}_p = \frac{(p^n - 1) \cdots (p^{n-m+1} - 1)}{(p^m - 1) \cdots (p - 1)}$$

(see, e.g., [22, Ch. 7]). It is also worth remarking that by changing the prime p to a variable q , one gets the quantum binomial coefficient $\begin{bmatrix} n \\ m \end{bmatrix}_q$ introduced by Gauss. Observe also that $\binom{n}{1}_p = \frac{p^n - 1}{p - 1}$.

Theorem 5.2. *Let p be an odd prime, and let \mathfrak{N} be the subspace of $J(F)$ defined above. Then*

$$\nu(M_{p^3}, F) = (p^2 - 1)\nu(H_{p^3}, F) + \left(\binom{\dim_{\mathbb{F}_p} J(F)}{1}_p - \binom{\dim_{\mathbb{F}_p} \mathfrak{N}}{1}_p \right) \frac{|J(F)|}{p^2}.$$

Before proving this result, we observe that when $\text{char}(F) \neq p$ then $|J(F)| < p^2$ is only possible when $p = 2$ and $n = 1$. Since we are focusing on the case $p > 2$, the term $|J(F)|/p^2$ is therefore an integer in this case. On the other hand, when $\text{char}(F) = p$ then $|J(F)| < p^2$ is possible, but in this case the term $\binom{\dim J(F)}{1}_p - \binom{\dim \mathfrak{N}}{1}_p$ vanishes.

Proof. Suppose that K/F is a G_1 -extension. From Proposition 3.4, we know that there is a bijection

$$\left\{ \begin{array}{l} \mathbb{F}_p[G_1] - \text{submodules} \\ M \subseteq J(K) \text{ with} \\ M \simeq A_2 \text{ and } M \subseteq \ker(e) \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{Solutions to} \\ H_{p^3} \twoheadrightarrow G_1 \\ \text{over } K/F \end{array} \right\}.$$

Now since any given module $M \simeq A_2$ satisfies $|\{m \in M : \ell(m) = 2\}| = p^2 - p$, and since any element $m \in J(K) \cap \ker(e)$ with $\ell(m) = 2$ generates a submodule corresponding to a solution to $H_{p^3} \twoheadrightarrow G_1$, we get

$$\nu(H_{p^3} \twoheadrightarrow G_1, K/F) = \frac{1}{p^2 - p} |\{\gamma \in J(K) \cap \ker(e) : \ell(\gamma) = 2\}|.$$

Since any H_{p^3} extension has $p + 1$ quotients isomorphic to \mathbb{Z}/p , we therefore conclude

$$\nu(H_{p^3}, F) = \frac{1}{p + 1} \sum_{K/F} \frac{1}{p^2 - p} |\{\gamma \in J(K) \cap \ker(e) : \ell(\gamma) = 2\}|.$$

Now we will consider M_{p^3} extensions, so again let K/F be a given G_1 -extension. We will fix an element χ as in Proposition 3.6. According to Proposition 3.4, we know that there is a bijection

$$\left\{ \begin{array}{l} \mathbb{F}_p[G_1] - \text{submodules} \\ M \subseteq J(K) \text{ with} \\ M \simeq A_2 \text{ and } M \not\subseteq \ker(e) \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{Solutions to} \\ M_{p^3} \twoheadrightarrow G_1 \\ \text{over } K/F \end{array} \right\}.$$

Again, any module $M \simeq A_2$ satisfies $|\{m \in M : \ell(m) = 2\}| = p^2 - p$, and if the module satisfies $M \not\subseteq \ker(e)$ then it must be that any element from $\{m \in M : \ell(m) = 2\}$ has $e(m) \neq 0$. (One can see this in several ways, but here's an embedding problem argument: if there were an element with $\ell(m) = 2$ and $e(m) = 0$, then $M = \langle m \rangle$ would solve $H_{p^3} \twoheadrightarrow G_1$ instead of $M_{p^3} \twoheadrightarrow G_1$.) Hence we conclude that

$$\nu(M_{p^3} \twoheadrightarrow G_1, K/F) = \frac{1}{p^2 - p} |\{\alpha \in J(K) : \alpha \notin \ker(e), \ell(\alpha) = 2\}|.$$

We claim that $\{\alpha \in J(K) : \alpha \notin \ker(e), \ell(\alpha) = 2\}$ is equal to

$$\begin{cases} \bigcup_{c=1}^{p-1} c\chi + \{\gamma \in J(K) \cap \ker(e) : \ell(\gamma) = 2\}, & \text{if } \ell(\chi) = 1 \\ \bigcup_{c=1}^{p-1} c\chi + \{\gamma \in J(K) \cap \ker(e) : \ell(\gamma) = 2\} \cup \bigcup_{c=1}^{p-1} c\chi + (J(K)^G \cap \ker(e)), & \text{if } \ell(\chi) = 2. \end{cases} \quad (8)$$

It will be convenient to translate these two conditions into equivalent statements: in the language of Proposition 3.6, the condition $\ell(\chi) = 1$ is equivalent to $i(K/F) = -\infty$, whereas in the language of embedding problem this condition says that $G_2 \twoheadrightarrow G_1$ is solvable over K/F . On the other hand, $\ell(\chi) = 2$ translates to $i(K/F) = 0$ in the language of Proposition 3.6, or to the embedding problem statement that $G_2 \twoheadrightarrow G_1$ does not have a solution over K/F .

If we assume the equality of sets from equation (8) for the time being, then since any given M_{p^3} -extension has a unique \mathbb{Z}/p -quotient, it will follow that

$$\begin{aligned} \nu(M_{p^3}, F) &= \sum_{K/F} \nu(M_{p^3} \twoheadrightarrow G_1, K/F) \\ &= \sum_{K/F} \frac{1}{p^2 - p} |\{\alpha \in J(K) : \alpha \notin \ker(e), \ell(\alpha) = 2\}| \\ &= \frac{p-1}{p^2 - p} \left(\sum_{K/F} |\{\gamma \in J(K) \cap \ker(e) : \ell(\gamma) = 2\}| + \sum_{i(K/F)=0} |J(K)^G \cap \ker(e)| \right) \\ &= (p^2 - 1)\nu(H_{p^3}, F) + \frac{1}{p} \sum_{i(K/F)=0} |J(K)^G \cap \ker(e)|. \end{aligned}$$

We connect this expression to the desired formula for $\nu(M_{p^3}, F)$ by considering two cases. First, suppose $\text{char}(F) = p$. In this case we have $i(K/F) = -\infty$ for any G_1 -extension K/F , and hence the latter sum is empty. But in this case note that the second summand from the desired formula for $\nu(M_{p^3}, F)$ also vanishes since $J(F) = \mathfrak{N}$ in this case. Hence

we have the desired result in this case. (Note: when $\xi_{p^2} \in F$ we also have $\mathfrak{N} = J(F)$ so that the latter term vanishes; this proves the other case of Brattström's result.)

Now suppose that $\text{char}(F) \neq p$. If K/F is a \mathbb{Z}/p -extension, let $\iota : J(F) \rightarrow J(K)$ be the map induced by the natural inclusion; from [31, Lemma 8] we have that $J(K)^G \cap \ker(e) = \iota(J(F))$, and from Kummer Theory we have that $|\iota(J(F))| = |J(F)|/p$. Hence we can continue our chain of equalities by writing

$$\nu(M_{p^3}, F) = (p^2 - 1)\nu(H_{p^3}, F) + \frac{|J(F)|}{p^2} |\{K/F : G_2 \twoheadrightarrow G_1 \text{ is not solvable}\}|.$$

The only thing left to argue, then, is that the number of extensions K/F for which $G_2 \twoheadrightarrow G_1$ is not solvable is given by $\binom{\dim J(F)}{1}_p - \binom{\dim \mathfrak{N}}{1}_p$, though this is straightforward given Proposition 5.1: $\binom{\dim J(F)}{1}_p$ counts all \mathbb{Z}/p -extensions, and $\binom{\dim \mathfrak{N}}{1}_p$ counts all \mathbb{Z}/p -extensions which admit a solution to the embedding problem $G_2 \twoheadrightarrow G_1$.

To finish the proof, then, we simply need to show that $\{\alpha \in J(K) : \alpha \notin \ker(e), \ell(\alpha) = 2\}$ is equal to the expression from equation (8). Suppose first that $\ell(\chi) = 1$. Let $\alpha \in J(K)$ be given which satisfies $e(\alpha) \neq 0$ and $\ell(\alpha) = 2$. Then there exists some $c \in \mathbb{F}_p^\times$ so that $\alpha - c\chi \in \ker(e)$, and the ultrametric property gives $\ell(\alpha - c\chi) = 2$. This gives one containment. For the other, if $\gamma \in J(K) \cap \ker(e)$ and $\ell(\gamma) = 2$, then the ultrametric property tells us that for any $c \in \mathbb{F}_p^\times$ we have $\ell(c\chi + \gamma) = 2$, and of course $e(c\chi + \gamma) \neq 0$.

Now suppose that $\ell(\chi) = 2$. Let $\alpha \in J(K)$ be given which satisfies $e(\alpha) \neq 0$ and $\ell(\alpha) = 2$. Then there exists some $c \in \mathbb{F}_p^\times$ so that $\alpha - c\chi \in \ker(e)$, though this time the ultrametric property only gives $\ell(\alpha - c\chi) \leq 2$. Hence either $\alpha - c\chi$ has length 2 or $\alpha - c\chi \in J(K)^G$. This proves one containment. For the other, the ultrametric property makes it clear that if $\gamma \in J(K)^G$ and $e(\gamma) = 0$, then for any $c \in \mathbb{F}_p^\times$ we have that $e(c\chi + \gamma) \neq 0$ and $\ell(c\chi + \gamma) = 2$. We claim that for $\gamma \in \ker(e)$ with $\ell(\gamma) = 2$, it is still true that for all $c \in \mathbb{F}_p^\times$ we have $e(c\chi + \gamma) \neq 0$ and $\ell(c\chi + \gamma) = 2$. The first statement is clear; for the second, note that if $\ell(c\chi + \gamma) < 2$ then this implies that $c\chi + \gamma$ is an element of nontrivial index with length 1, a contradiction to the fact that χ is an element of nontrivial index with minimal length. \square

Notice that in the previous theorem we had to be careful in using our methodology to enumerate extensions since our modules naturally parameterize solutions to embedding problems over a given \mathbb{Z}/p -extension K/F . In the case of H_{p^3} extensions of F , we had to account for the fact that a given H_{p^3} extension of F solves embedding problems over $p+1$ distinct \mathbb{Z}/p -extension of F . To adopt the methodology of the previous theorem to a broader class of groups, we will be interested in determining when groups of the form $A_i \rtimes G_n$ or $A_i \bullet G_n$ have precisely one normal subgroup which is elementary p -abelian and whose quotient is isomorphic \mathbb{Z}/p^n .

Lemma 5.3. *Suppose that $\text{Gal}(L/F) \simeq A_i \rtimes G_n$ for $i \geq p^{n-1} + 2$. Then there is a unique intermediate \mathbb{Z}/p^n -extension K/F so that L/K is elementary p -abelian. Likewise if $\text{Gal}(L/F) \simeq A_i \bullet G_n$ for $i \geq p^{n-1} + 1$, then there is a unique intermediate \mathbb{Z}/p^n -extension K/F so that L/K is elementary p -abelian.*

Proof. In each case, it is obvious that $T = \{(f, 1) : f \in A_i\}$ is a normal subgroup which is elementary p -abelian. Equally clear is that the fixed field is a \mathbb{Z}/p^n -extension. Before

proceeding, we observe that the collection of elements in $A_i \rtimes G_n$ with order p are those of the form (f, σ^j) where $p^{n-1} \mid j$.

For the sake of contradiction, suppose that $H \neq T$ is an elementary p -abelian normal subgroup of $A_i \rtimes G_n$ with quotient \mathbb{Z}/p^n ; this forces $|H| = p^i$ and $H \setminus T \neq \emptyset$. Choose $(f, \sigma^j) \in H \setminus T$ so that $\ell(f)$ is maximal amongst elements within $H \setminus T$. After taking a suitable power of (f, σ^j) if necessary, we can assume that our element is $(f, \sigma^{p^{n-1}})$. (Note that $(f, \sigma^j)^t = (\sum_{i=0}^{t-1} \sigma^{it} f, \sigma^{jt})$, and that $\sum_{k=0}^{t-1} \sigma^{jk}$ is a unit in $\mathbb{F}_p[G]$ for $1 \leq t \leq p-1$, so that $\ell(f) = \ell(\sum_{k=0}^{t-1} \sigma^{jk} f)$.)

Since H is normal we know that the commutator $[(0, \sigma), (f, \sigma^j)] = ((\sigma - 1)f, 1)$ is an element of H ; repeating this procedure shows $\{(g, 1) : \ell(g) < \ell(f)\} \subseteq H$. By the maximality of $(f, \sigma^{p^{n-1}})$, there exists no $(g, \sigma^k) \in H$ with $k \neq p^n$ and $\ell(g) > \ell(f)$. We argue that there are also no elements $(g, 1) \in H$ with $\ell(g) > \ell(f)$; otherwise $(h, 1)(f, \sigma^{p^{n-1}}) = (h + f, \sigma^{p^{n-1}}) \in H$, and the ultrametric property gives $\ell(h + f) = \ell(h)$, violating the maximality condition defining f . Notice also that since $((\sigma - 1)f, 1) \in H$ and H is assumed abelian, we must have

$$(f + (\sigma - 1)f, \sigma^{p^{n-1}}) = ((\sigma - 1)f, 1)(f, \sigma^{p^{n-1}}) = (f, \sigma^{p^{n-1}})((\sigma - 1)f, 1) = (f + \sigma^{p^{n-1}}(\sigma - 1)f, \sigma^{p^{n-1}}).$$

It therefore follows that $(\sigma - 1)f$ is fixed by $\sigma^{p^{n-1}}$, and so $\ell(f) \leq p^{n-1} + 1$.

Now suppose that H contains no elements of the form (g, σ^k) with $k \neq p^n$ and $\ell(g) < \ell(f)$. Then we have

$$H = \left\langle (f, \sigma^{p^{n-1}}), ((\sigma - 1)f, 1), ((\sigma - 1)^2 f, 1), \dots, ((\sigma - 1)^{\ell(f)-1} f, 1) \right\rangle_{\mathbb{F}_p},$$

and hence $|H| = p^{\ell(f)} \leq p^{p^{n-1}+1} < p^i$, a contradiction.

On the other hand, suppose that H does contain an element (g, σ^k) with $k \neq p^n$ and $\ell(g) < \ell(f)$. One can argue that (g, σ^k) can be chosen to take the form $(g, \sigma^{p^{n-1}})$ as before, and since we have already established $(g, 1) \in H$, we conclude that $(0, \sigma^{p^{n-1}}) \in H$. This gives $(f, \sigma^{p^{n-1}})(0, \sigma^{p^{n-1}})^{-1} = (f, 1) \in H$ as well. The commutivity of H implies

$$(f, \sigma^{p^{n-1}}) = (f, 1)(0, \sigma^{p^{n-1}}) = (0, \sigma^{p^{n-1}})(f, 1) = (\sigma^{p^{n-1}} f, \sigma^j).$$

We conclude that f is fixed by the action of $\sigma^{p^{n-1}}$, so that in fact $\ell(f) \leq p^{n-1}$ in this case. But then

$$H = \left\langle (f, 1), ((\sigma - 1)f, 1), \dots, ((\sigma - 1)^{\ell(f)-1} f, 1), (0, \sigma^{p^{n-1}}) \right\rangle_{\mathbb{F}_p},$$

contradicting the fact that $i \geq p^{n-1} + 2$ in this case. This completes the proof for $A_i \rtimes G_n$.

Now suppose that $H \neq T$ is an elementary p -abelian normal subgroup of $A_i \bullet G_n$ with quotient \mathbb{Z}/p^n ; this forces $|H| = p^i$. Again, we will choose $(f, \sigma^j) \in H \setminus T$ so that $\ell(f)$ is maximal amongst elements within $H \setminus T$, and we again observe that we can assume that this element is of the form $(f, \sigma^{p^{n-1}})$. We begin our argument in this case by claiming that $\ell(f) > p^n - p^{n-1}$ is necessary. To do so, we first establish some notation. For an integer a , we write \bar{a} for the least non-negative residue of a modulo p^n . For $m \in \mathbb{N}$, we then define

$c_j(m)$ inductively: $c_j(1) = 0$, and

$$c_j(m+1) = \begin{cases} c_j(m) & \text{if } \overline{mj} + j < p^n \\ c_j(m) + 1 & \text{if } \overline{mj} + j \geq p^n. \end{cases}$$

Then one can use induction to show that

$$(f, \sigma^{p^{n-1}})^m = \left(\sum_{k=0}^{m-1} \sigma^{kp^{n-1}} f + c_{p^{n-1}}(m)(\sigma - 1)^{i-1}, \sigma^{mp^{n-1}} \right).$$

Take $m = p$ and observe that $1 \leq c_{p^{n-1}}(p) < p$ (the first inequality follows because $p^{n-1}p \geq p^n$, and the latter because $c_{p^{n-1}}(1) = 0$ and $c_{p^{n-1}}(m+1) - c_{p^{n-1}}(m) \leq 1$ for all m). If $\ell(f) \leq p^{n-1}(p-1)$ this means that

$$\begin{aligned} (f, \sigma^{p^{n-1}})^p &= \left(\sum_{k=0}^{p-1} \sigma^{kp^{n-1}} f + c_{p^{n-1}}(p)(\sigma - 1)^{i-1}, 1 \right) \\ &= \left((\sigma^{p^{n-1}} - 1)^{p-1} f + c_{p^{n-1}}(p)(\sigma - 1)^{i-1}, 1 \right) = (c_{p^{n-1}}(p)(\sigma - 1)^{i-1}, 1) \neq (0, 1), \end{aligned}$$

contrary to the assumption that H is elementary p -abelian.

Now observe that $[(0, \sigma), (f, \sigma^{p^{n-1}})] \in H$, and hence should commute with $(f, \sigma^{p^{n-1}})$. But a computation reveals

$$[(f, \sigma^{p^{n-1}}), [(0, \sigma), (f, \sigma^{p^{n-1}})]] = ((\sigma - 1)(\sigma^{p^{n-1}} - 1)f, 1).$$

Provided either $p > 3$ or $n = 1$, this element is nontrivial because $\ell(f) \geq p^n - p^{n-1} > p^{n-1} + 1$, and so H is not commutative.

We will handle the remaining case $p = 3$ and $n = 1$ directly. We have the group $A_i \bullet \mathbb{Z}/3\mathbb{Z}$, where $2 \leq i \leq 3$, and we want to show this group has a unique \mathbb{Z}/p -quotient whose corresponding normal subgroup is $\mathbb{Z}/p \times \mathbb{Z}/p$. When $i = 2$ then the group is simply M_{33} , and we already know the result for this group. When $i = 3$ then $A_i \bullet \mathbb{Z}/3 \simeq A_i \rtimes \mathbb{Z}/3$, and we have already established the desired result from the first part of this theorem. \square

Theorem 5.4. *For an extension $K/F \simeq \mathbb{Z}/p^n$ and $p^{n-1} + 2 \leq i < p^n$,*

$$\nu(A_i \bullet G_n \twoheadrightarrow G_n, K/F) = (p-1)\nu(A_i \rtimes G_n \twoheadrightarrow G_n, K/F).$$

Moreover, for a field F and $p^{n-1} + 2 \leq i < p^n$,

$$\nu(A_i \bullet G_n, F) = (p-1)\nu(A_i \rtimes G_n, F).$$

Proof. We begin by noting that Lemma 5.3 tells us that the second statement follows from the first, since a given $A_i \rtimes G_n$ or $A_i \bullet G_n$ extension of F has a unique \mathbb{Z}/p^n -subextension K/F such that L/K is elementary p -abelian. Hence such an extension is parameterized uniquely as a module within $J(K)$, and so we have

$$\nu(A_i \rtimes G_n, F) = \sum_{\text{Gal}(K/F) \simeq G_n} \nu(A_i \rtimes G_n \twoheadrightarrow G_n, K/F)$$

and likewise for the non-semidirect product. Hence, we will focus on proving the first result.

To do so, we note that using Proposition 3.4 and that fact that any cyclic module of dimension i has $p^i - p^{i-1}$ many generators, one has

$$\begin{aligned}\nu(A_i \rtimes G_n \twoheadrightarrow G_n, K/F) &= \frac{1}{p^i - p^{i-1}} |\{\gamma \in J(K) : \gamma \in \ker(e), \ell(\gamma) = i\}| \\ \nu(A_i \bullet G_n \twoheadrightarrow G_n, K/F) &= \frac{1}{p^i - p^{i-1}} |\{\alpha \in J(K) : \alpha \notin \ker(e), \ell(\alpha) = i\}|.\end{aligned}$$

The desired result will follow if we can show that, for the element $\chi \in J(K)$ from Proposition 3.6, one has

$$\{\alpha \in J(K) : \alpha \notin \ker(e), \ell(\alpha) = i\} = \bigcup_{c=1}^{p-1} c\chi + \{\gamma \in J(K) : \gamma \in \ker(e), \ell(\gamma) = i\}.$$

For this, note that $\ell(\chi) = p^{i(E/F)} + 1 < i$, and so if $\ell(\gamma) = i$ then the ultrametric property gives $\ell(c\chi + \gamma) = i$. Of course if $\gamma \in \ker(e)$ as well, then $e(c\chi + \gamma) \neq 0$. This gives one containment. For the other, note that if $\alpha \notin \ker(e)$ then there exists some $c \in \mathbb{F}_p^\times$ so that $\alpha - c\chi \in \ker(e)$; when $\ell(\alpha) = i$, the ultrametric property again gives $\ell(\alpha - c\chi) = i$, and hence $\alpha = c\chi + \alpha - c\chi \in c\chi + \{\gamma \in J(K) : \gamma \in \ker(e), \ell(\gamma) = i\}$. \square

If one is willing to settle for counting only solutions to embedding problems, one can extend these same ideas to express $\nu(A_\ell \rtimes G_1 \twoheadrightarrow G_1, K/F)$ in terms of $\nu(H_{p^3} \twoheadrightarrow G_1, K/F)$ and $\nu(\mathbb{Z}/p \times \mathbb{Z}/p \twoheadrightarrow \mathbb{Z}/p, K/F)$.

Theorem 5.5. *For $2 \leq \ell \leq p-1$ and a \mathbb{Z}/p -extension K/F , we have*

$$\begin{aligned}\nu(A_\ell \rtimes \mathbb{Z}/p \twoheadrightarrow \mathbb{Z}/p, K/F) \\ = \nu(H_{p^3} \twoheadrightarrow \mathbb{Z}/p, K/F) \left(\frac{1}{p} + \frac{(p-1)\nu(H_{p^3} \twoheadrightarrow \mathbb{Z}/p, K/F)}{1 + (p-1)\nu(\mathbb{Z}/p \times \mathbb{Z}/p \twoheadrightarrow \mathbb{Z}/p, K/F)} \right)^{\ell-2}.\end{aligned}$$

Proof. We know that

$$\nu(H_{p^3} \twoheadrightarrow \mathbb{Z}/p, K/F) = \frac{1}{p^2 - p} |\{\gamma \in J(K) : \ell(\gamma) = 2 \text{ and } \gamma \in \ker(e)\}|.$$

Likewise we have

$$\nu(A_\ell \rtimes \mathbb{Z}/p \twoheadrightarrow \mathbb{Z}/p, K/F) = \frac{1}{p^\ell - p^{\ell-1}} |\{\gamma \in J(K) : \ell(\gamma) = \ell \text{ and } \gamma \in \ker(e)\}|.$$

By Proposition 3.6 we know that the $\mathbb{F}_p[G_1]$ -structure of $\ker(e)$ is

$$\ker(e) \simeq \bigoplus_{\mathfrak{d}_0} \mathbb{F}_p \oplus \bigoplus_{\mathfrak{d}_1} \mathbb{F}_p[G_1]/(\sigma - 1)^{p-2}.$$

Hence it is relatively simply to see that for $1 \leq \ell \leq p-1$ we have

$$|\{\gamma \in J : \ell(\gamma) \leq \ell \text{ and } \gamma \in \ker(e)\}| = p^{\mathfrak{d}_0 + \ell \mathfrak{d}_1}.$$

Hence for $2 \leq \ell \leq p-1$ we have

$$|\{\gamma \in J : \ell(\gamma) = \ell \text{ and } \gamma \in \ker(e)\}| = p^{\mathfrak{d}_0 + \ell \mathfrak{d}_1} - p^{\mathfrak{d}_0 + (\ell-1)\mathfrak{d}_1} = p^{\mathfrak{d}_0 + (\ell-1)\mathfrak{d}_1} (p^{\mathfrak{d}_1} - 1)$$

and for $\ell = 1$ we get

$$|\{\gamma \in J : \ell(\gamma) = 1 \text{ and } \gamma \in \ker(e)\}| = p^{\mathfrak{d}_0 + \mathfrak{d}_1} - 1.$$

Hence for $2 \leq \ell \leq p-1$, one calculates

$$\begin{aligned} \nu(A_\ell \rtimes \mathbb{Z}/p \twoheadrightarrow \mathbb{Z}/p, K/F) &= \frac{1}{p^\ell - p^{\ell-1}} |\{\gamma \in \ker(e) : \ell(\gamma) = \ell\}| \\ &= \frac{1}{p^{\ell-1}(p-1)} p^{\mathfrak{d}_0 + (\ell-1)\mathfrak{d}_1} (p^{\mathfrak{d}_1} - 1) \\ &= p^{\mathfrak{d}_0 + \mathfrak{d}_1 - 1} \frac{p^{\mathfrak{d}_1} - 1}{p-1} (p^{\mathfrak{d}_1 - 1})^{\ell-2}. \end{aligned} \quad (9)$$

Of course the case $\ell = 1$ follows in a similar way:

$$\nu(\mathbb{Z}/p \times \mathbb{Z}/p \twoheadrightarrow \mathbb{Z}/p, K/F) = \frac{p^{\mathfrak{d}_0 + \mathfrak{d}_1} - 1}{p-1}. \quad (10)$$

Because it will be particularly useful in a moment, let us also note that

$$\nu(H_{p^3} \twoheadrightarrow \mathbb{Z}/p, K/F) = p^{\mathfrak{d}_0 + \mathfrak{d}_1 - 1} \frac{p^{\mathfrak{d}_1} - 1}{p-1}. \quad (11)$$

One can solve for $p^{\mathfrak{d}_0 + \mathfrak{d}_1}$ and $p^{\mathfrak{d}_1}$ using equations (10) and (11), and ultimately recover

$$\begin{aligned} p^{\mathfrak{d}_0 + \mathfrak{d}_1} &= 1 + (p-1)\nu(\mathbb{Z}/p \times \mathbb{Z}/p \twoheadrightarrow \mathbb{Z}/p, K/F) \\ p^{\mathfrak{d}_1} &= 1 + \frac{p(p-1)}{p^{\mathfrak{d}_0 + \mathfrak{d}_1}} \nu(H_{p^3} \twoheadrightarrow \mathbb{Z}/p, K/F) \\ &= 1 + \frac{p(p-1)\nu(H_{p^3} \twoheadrightarrow \mathbb{Z}/p, K/F)}{1 + (p-1)\nu(\mathbb{Z}/p \times \mathbb{Z}/p \twoheadrightarrow \mathbb{Z}/p, K/F)} \end{aligned}$$

With these in hand, we can reexpress (9) to satisfy the statement of the Proposition:

$$\begin{aligned} \nu(A_\ell \rtimes \mathbb{Z}/p \twoheadrightarrow \mathbb{Z}/p, K/F) &= p^{\mathfrak{d}_0 + \mathfrak{d}_1 - 1} \frac{p^{\mathfrak{d}_1} - 1}{p-1} (p^{\mathfrak{d}_1 - 1})^{\ell-2} \\ &= \nu(H_{p^3} \twoheadrightarrow \mathbb{Z}/p, K/F) \left(\frac{1}{p} + \frac{(p-1)\nu(H_{p^3} \twoheadrightarrow \mathbb{Z}/p, K/F)}{1 + (p-1)\nu(\mathbb{Z}/p \times \mathbb{Z}/p \twoheadrightarrow \mathbb{Z}/p, K/F)} \right)^{\ell-2}. \end{aligned}$$

□

We finish with some realization multiplicity results for groups from the family $A_i \rtimes G_1$ and $A_i \bullet G_1$. The realization multiplicity of G , written $\nu(G)$, is the minimal positive value for $\nu(G, F)$ as F ranges over all fields; likewise, the realization multiplicity for an embedding problem $G \twoheadrightarrow Q$, written $\nu(G \twoheadrightarrow Q)$, is the minimal positive value for $\nu(G \twoheadrightarrow Q, K/F)$ as K/F ranges over all fields with $\text{Gal}(K/F) \simeq Q$. There are very few realization multiplicity results known for nonabelian p -groups; the known results come from [20] and are $\nu(M_{p^3}) = p$, $\nu(M_{p^3} \times \mathbb{Z}/p) = p^2 - 1$, and $\nu((\mathbb{Z}/p)^k \times H_{p^3}) = 1$ for $k \in \mathbb{Z}_{\geq 0}$.

Example 5.6. Consider a field F with $\text{char}(F) \neq p$ and $\dim_{\mathbb{F}_p}(J(F)) = 2$ and such that $G_F := \text{Gal}(F_{\text{sep}}/F)$ is the free pro- p group on two generators. (Such a field exists as seen in [14, Cor. 23.1.2].) Now we claim that $\xi_p \in F$, since otherwise we would have $F(\xi_p) \subseteq F_{\text{sep}}$

and $1 < [F(\xi_p) : F] \leq p-1 < p$. But this would imply that G_F has a quotient whose order was not a power of p , a clear contradiction.

Since G_F is a free pro- p group we have $H^2(F) = 0$, and therefore $(f_1) \cup (f_2) = 0$ for each $f_1, f_2 \in J(F)$. But then we conclude that $f_1 \in N_{F(\sqrt[p]{f_2})/F}(F(\sqrt[p]{f_2}))$ for all $f_1, f_2 \in F^\times$. Suppose, then, that f_1, f_2 are generators for $J(F)$. If we let $\alpha \in F(\sqrt[p]{f_2})$ be given so that $N_{F(\sqrt[p]{f_2})/F}(\alpha) = f_1$, and if we write σ for the generator of the G_1 -extension $F(\sqrt[p]{f_2})/F$, then $\hat{\alpha} = \alpha^{(\sigma-1)^{p-2}}$ has $\ell(\hat{\alpha}) = 2$ and $e(\hat{\alpha}) = 0$. Hence $\langle \hat{\alpha} \rangle$ corresponds to a solution to the embedding problem $H_{p^3} \twoheadrightarrow \mathbb{Z}/p$.

Corollary 5.7.

- (1) $\nu(H_{p^3}) = 1$;
- (2) $\nu(A_p \rtimes \mathbb{Z}/p) = p^2 - 1$
- (3) $\nu(A_i \rtimes \mathbb{Z}/p) = p + 1$ for $2 < i < p - 1$
- (4) $\nu(A_i \bullet \mathbb{Z}/p) = p^2 - 1$ for $2 < i < p - 1$; and

Remark. Though it is already known, we reprove statement (1) for two reasons: to again showcase a module-theoretic perspective, and because statement (1) provides the necessary example in proving statements (2-4).

Proof. Statement (1) is a consequence of Example 5.6. In that example we are told that there is a \mathbb{Z}/p -extension K/F for which the embedding problem $H_{p^3} \twoheadrightarrow \mathbb{Z}/p$ is solvable; call this H_{p^3} -extension L/F . Combined with the fact that $\ker |J(F) \rightarrow J(K)| = p$, one can use this to show that $J(K) \simeq X \oplus \mathbb{F}_p[G_1]$, with $\dim_{\mathbb{F}_p}(X) = 1$. But note that in fact L/F is solution to the embedding problem $H_{p^3} \twoheadrightarrow \mathbb{Z}/p$ for *any* \mathbb{Z}/p -extension \tilde{K}/F , from which we can deduce that $J(\tilde{K}) \simeq J(K)$. Hence over each \mathbb{Z}/p -extension of F there is a unique module isomorphic to A_2 and generated by an element of trivial index. Each of these modules corresponds to the same H_{p^3} -extension L/F .

One can also prove this result by thinking of H_{p^3} as an extension of $\mathbb{Z}/p \times \mathbb{Z}/p$ by \mathbb{Z}/p . Consider the field F from Example 5.6 again, and note that F has a unique $\mathbb{Z}/p \times \mathbb{Z}/p$ -extension K . Because any H_{p^3} -extension of F contains a unique $\mathbb{Z}/p \times \mathbb{Z}/p$ quotient extension over F , we see that any H_{p^3} -extension of F contains K/F . Now recall that [21, Thm. 6.6.1] tells us that if $K = F(\sqrt[p]{a}, \sqrt[p]{b})$, and if $w \in F(\sqrt[p]{a})$ is an element so that $L = F(\sqrt[p]{w}, \sqrt[p]{b})$ is an H_{p^3} -extension of F , then all other solutions to the H_{p^3} embedding problem over K/F take the form $L_f := K(\sqrt[p]{fw}, \sqrt[p]{b})$. But notice that since K/F is the unique $\mathbb{Z}/p \times \mathbb{Z}/p$ -extension of F , we have $\sqrt[p]{f} \in K$; it follows that $L_f = L$, and so F has a unique H_{p^3} -extension.

The proofs of statements (2-4) are all relatively similar and use Example 5.6 to establish upper bounds; we will prove (2) and leave the verification of the other two statements to the reader. So let F be the field from Example 5.6, and note that for each \mathbb{Z}/p -extension K/F there are p modules isomorphic to A_p . Each of these corresponds to a distinct solution to the embedding problem $A_p \rtimes G_1 \twoheadrightarrow G_1$. By Lemma 5.3, the solutions to this embedding problem over each of the \mathbb{Z}/p -extensions of F are distinct. Hence we have $\nu(A_p \rtimes G_1) \leq p^2 + p$.

For the lower bound, observe that if there is a single $A_p \rtimes G_1$ -extension of a field F , then the \mathbb{Z}/p -subextension K/F corresponding to the natural projection $A_p \rtimes G_1 \twoheadrightarrow G_1$ has the property that $J(K)$ contains a module $\langle \gamma \rangle$ isomorphic to A_p . If we choose an element χ as in Proposition 3.6, then each of the modules $\langle \gamma + c\chi \rangle$ for $c \in \{0, 1, \dots, p-1\}$ are also isomorphic to A_p . Observe additionally that any of the p other \mathbb{Z}/p -extensions of F admit a solution to the embedding problem $A_2 \rtimes G_1$ (i.e., the H_{p^3} subextension from the original $A_p \rtimes G_1$ extension), and hence by Proposition 4.1(1) also admits at least one solution to the embedding problem $A_p \rtimes G_1 \twoheadrightarrow G_1$. Since we have already argued that one such solution forces the appearance of p solutions, this tells us that F must have at least $p^2 + p$ extensions with Galois group $A_p \rtimes G_1$. \square

REFERENCES

- [1] F. ANDERSON, K. FULLER. *Rings and categories of modules*. Graduate Texts in Mathematics 13. New York: Springer-Verlag, 1973.
- [2] F. BERTRANDIAS, J.J. PAYAN. Γ -extensions et invariants cyclotomiques. *Ann.Scient.Ec.Norm.Sup.*, **5** (1972), no. 4, 517–543.
- [3] F. BOGOMOLOV, Y. TSCHINKEL. Universal spaces for unramified Galois cohomology. Available at <http://www.math.nyu.edu/~tschinke/papers/yuri/14bloch/bloch18.pdf>. To appear in Brauer groups and obstructions problems: moduli spaces and arithmetic, (A. Auel, B. Hassett, A. Varilly-Alvarado, and B. Viray eds.), (2014).
- [4] F. BOGOMOLOV, Y. TSCHINKEL. Commuting elements in Galois groups of function fields. In *Motives, polylogarithms and Hodge theory*, edited by F. Bogomolov, L. Katzarkov. International Press (2002), 75–120.
- [5] F. BOGOMOLOV, Y. TSCHINKEL. Introduction to birational anabelian geometry. In *Current developments in algebraic geometry*, edited by L. Caporaso, J. McKernan, M. Mustata, M. Popa, volume 59 of MSRI Publications, Cambridge University Press (2012), 17–63.
- [6] G. BRATTSTRÖM. On p -groups as Galois groups. *Math. Scandinavica* **65** (1989), no. 2, 165–174.
- [7] S. CHEBOLU, I. EFRAT, J. MINÁČ. Quotients of absolute Galois groups which determine the entire Galois cohomology. *Math. Annalen*. **352** (2012), no. 1, 205–221.
- [8] D. DUMMIT, R. FOOTE. *Abstract algebra, 2nd ed.* Upper Saddle River, NJ: Prentice Hall, 1999.
- [9] I. EFRAT. The Zassenhaus filtration, Massey products, and representations of profinite groups. *Adv. Math* **263** (2014), 389–411.
- [10] I. EFRAT. Filtrations of free groups as intersections. *Arch. Math. (Basel)* **103** (2014), no. 5, 411–420. Available at <http://arxiv.org/pdf/1312.1811>.
- [11] I. EFRAT, J. MINÁČ. On the descending central sequence of absolute Galois groups. *Amer. J. Math.*, **133** (2011), 1503–1532.
- [12] I. EFRAT, J. MINÁČ. Galois groups and cohomological functors. *Trans. Amer. Math. Soc.* (2016), <http://dx.doi.org/10.1090/tran/6724>, in press. Available at <http://arxiv.org/abs/1103.1508>.
- [13] I. EFRAT, J. MINÁČ. Small Galois groups that encode valuations. *Acta. Arith.* **156** (2012), no. 1, 7–17.
- [14] M. FRIED, M. JARDEN. *Field Arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol. 11. Berlin: Springer Berlin Heidelberg, 2005.
- [15] P. GILLE, T. SZAMUELY. *Central simple algebras and Galois cohomology*. Cambridge studies in advanced mathematics 101, Cambridge University Press, 2006.
- [16] M. HALL. *The theory of groups*. Macmillan Company, New York, 1959.
- [17] M. HOPKINS, K. WICKELGREN. Splitting varieties for triple Massey products. *J. Pure Appl. Algebra*, **219** (2015), no. 5, 1304–1319. Available at <http://arxiv.org/pdf/1210.4964>.
- [18] V.V. ISHKHANOV, B.B. LUR’E, D.K. FADDEEV. *The embedding problem in Galois theory*. Translations in mathematical monographs, vol. 165. Amer. Math. Soc., Providence, 1997.
- [19] C. U. JENSEN. On the representations of a group as a Galois group over an arbitrary field. *Théorie des nombres* (Quebec, PQ, 1987), 441–458. Berlin: de Gruyter, 1989.

- [20] C.U. JENSEN. Finite groups as Galois groups over arbitrary fields. Proceedings of the International Conference on Algebra, Part 2 (Novosibirsk, 1989), 435–448. Contemp. Math. **131**, Part 2. Providence, RI: American Mathematical Society, 1992.
- [21] C.U. JENSEN, A. LEDET, N. YUI. *Generic polynomials: constructive aspects of the inverse Galois problem*. Mathematical Sciences Research Institute Publications 45. Cambridge: Cambridge University Press, 2002.
- [22] V. KAC, P. CHEUNG. Quantum calculus. Springer, 2002.
- [23] S. LANG. *Algebra*, 3rd ed. Graduate texts in mathematics, 211. Springer, 2005.
- [24] A. LEDET. Brauer type embedding problems. Fields Institute Monographs 21. Providence, RI: AMS, 2005.
- [25] N. LEMIRE, J. MINÁČ, A. SCHULTZ, J. SWALLOW. Galois module structure of Galois cohomology for embeddable cyclic extensions of degree p^n . *J. London Math. Soc.* **81** (2010), no. 3, 525–543.
- [26] R. MASSY. Construction de p -extensions Galoisiennes d'un corps de caractéristique différente de p . *J. Algebra* **109** (1987), 508–535.
- [27] I. MICHAILOV. Induced orthogonal representations of Galois groups. *J. Alg.* **322** (2009), 3713–3732.
- [28] I. MICHAILOV. Four non-abelian groups of order p^4 as Galois groups. *J. Alg.* **307** (2007), 287–299.
- [29] J. MILNOR. Algebraic K -theory and quadratic forms. *Inventiones Math.* **9** (1970), 318–344.
- [30] J. MINÁČ, M. ROGELSTAD, N.D. TAN. Dimensions of Zassenhaus filtration subquotients of some pro- p -groups. *Israel J. Math.* **212** (2016), no. 2, 825–855. Available at <http://arxiv.org/pdf/1405.6980>.
- [31] J. MINÁČ, A. SCHULTZ, J. SWALLOW. Galois module structure of the p th-power classes of cyclic extensions of degree p^n . Proc. London Math. Soc. **92** (2006), no. 2, 307–341.
- [32] J. MINÁČ, A. SCHULTZ, J. SWALLOW. Automatic realizations of Galois groups with cyclic quotient of order p^n . *J. Théor. Nombres Bordeaux* **20** (2008), 419–430.
- [33] J. MINÁČ, M. SPIRA. Witt rings and Galois groups. *Ann. Math.* **144** (1996), 36–60.
- [34] J. MINÁČ, M. SPIRA. Formally real fields, Pythagorean fields, C -fields and W -groups. *Math. Z.* **205** (1990), 519–530.
- [35] J. MINÁČ, J. SWALLOW. Galois embedding problems with cyclic quotient of order p . *Israel J. Math.* **145** (2005), 93–112.
- [36] J. MINÁČ, N.D. TAN. Triple Massey products over global fields. *Doc. Math.* **20** (2015), 1467–1480. Available at <http://arxiv.org/abs/1403.4586>.
- [37] J. MINÁČ, N.D. TAN. Triple Massey products and Galois theory. *J. Eur. Math. Soc. (JEMS)* (2016), in press. Available at <http://arxiv.org/abs/1307.6624>.
- [38] J. MINÁČ, N.D. TAN. The kernel unipotent conjecture and the vanishing of Massey products of odd rigid fields. (With an appendix by I. EFRAT, J. MINÁČ, and N.D. TAN.) *Adv. Math.* **273** (2015), 242–270. Available at <http://arxiv.org/abs/1312.2655>.
- [39] J. NEUKIRCH, A. SCHMIDT, K. WINGBERG. *Cohomology of Number Fields*, 2nd ed. Berlin: Springer-Verlag, 2008.
- [40] A. PFISTER. Eine Bemerkung zum normenresthomomorphismus $h : K^*F/2 \rightarrow H^*(F, \mathbb{Z}/2)$. *Arch. Math.* **81** (2003), 272–284.
- [41] A. PFISTER. On the Milnor conjectures: history, influence, applications. *Jber. d. Dt. Math-Verein.* **102** (2000), 15–41.
- [42] R.C. PIERCE. Associative algebras. Graduate Texts in Mathematics, Vol. 88. Springer-Verlag, 1982.
- [43] F. POP. On Grothendieck's conjecture of birational anabelian geometry. *Ann. of Math.* **139** (1994), 145–182.
- [44] F. POP. On the birational program initiated by Bogomolov I. *Invent. Math.* **187** (2012), 511–533.
- [45] A. SCHULTZ. Parameterizing solutions to any Galois embedding problem over $\mathbb{Z}/p^n\mathbb{Z}$ with elementary p -abelian kernel. *J. Algebra* **411** (2014), 50–91.
- [46] I.R. SHAFAREVICH. Construction of fields of algebraic number fields with given solvable groups (in Russian). *Izv. Akad. Nauk SSSR* **18** (1954), no. 6, 525–578. English translation in *Amer. Math. Soc. Transl.* **4** (1956), 185–237.
- [47] I.R. SHAFAREVICH. Factors of a decreasing central series (in Russian). *Mat. Zametki* **45** (1989), 114–117. English transition in *Math. Notes* **45** (1989), 262–264.

- [48] I.R. SHAFAREVICH. On the construction of fields with a given Galois group of order ℓ^α (in Russian). *Izv. Akad. Nauk SSSR* **18** (1954), 261–296. English transition in *Amer. Mat. Soc. Transl.* **4** (1956), 107–142.
- [49] V. SRINIVAS. *Algebraic K-theory*, reprint of 2nd ed. Part of *Modern Birkhäuser classics*. Boston, MA: Birkhäuser, 2008.
- [50] A. TOPAZ. Abelian-by-central Galois groups of fields I: a formal description. To appear in *Trans. Amer. Math. Soc.* Available at <http://arxiv.org/pdf/1310.5613>.
- [51] A. TOPAZ. Commuting-liftable subgroups of Galois groups II. To appear in *J. Reine Angew. Math.* Available at <http://arxiv.org/pdf/1208.0583>.
- [52] V. VOEVODSKY. On motivic cohomology with \mathbf{Z}/l -coefficients. **174** (2011), 401–438.
- [53] W. WATERHOUSE. The normal closures of certain Kummer extensions. *Canad. Math. Bull.* **37** (1994), no. 1, 133–139.
- [54] G. WHAPLES. Algebraic extensions of arbitrary fields. *Duke Math. J.* **24** (1957), 201–204.
- [55] E. WITT. Konstruktion von galoisschen körpern der charakteristik p zu vorgegebener gruppe der ordnung p^f . *J. Reine Angew. Math.* **174** (1936), 237–245.

DEPARTMENT OF MATHEMATICS, ILLINOIS STATE UNIVERSITY, CAMPUS BOX 4520, NORMAL, IL 61790 USA

E-mail address: `schebol@ilstu.edu`

DEPARTMENT OF MATHEMATICS, MIDDLESEX COLLEGE, UNIVERSITY OF WESTERN ONTARIO, LONDON, ONTARIO N6A 5B7 CANADA

E-mail address: `minac@uwo.ca`

DEPARTMENT OF MATHEMATICS, WELLESLEY COLLEGE, 106 CENTRAL STREET, WELLESLEY, MA 01702 USA

E-mail address: `andrew.c.schultz@gmail.com`